N° d'ordre : 2011-21-TH

THÈSE DE DOCTORAT

SPÉCIALITÉ : PHYSIQUE

École Doctorale « Sciences et Technologies de l'Information des Télécommunications et des Systèmes »

Présentée par :

Joffrey VILLARD

Sujet :

CODAGE DE SOURCE CIBLÉ : TRANSMISSION SÉCURISÉE, DÉTECTION

TASK–ORIENTED SOURCE CODING: SECURE TRANSMISSION, DETECTION

Soutenue le jeudi 1er décembre 2011 devant les membres du jury :

Prof. Giuseppe CAIRE	University of Southern California	Rapporteur
Prof. H. Vincent POOR	Princeton University	Rapporteur
Dr. Pierre DUHAMEL	L2S CNRS/SUPELEC/Univ. Paris-Sud 11	Examinateur
Dr. Olivier RIOUL	Institut Télécom/Télécom ParisTech/CNRS LTCI	Examinateur
Prof. Mikael SKOGLUND	KTH Royal Institute of Technology	Examinateur
Dr. Pascal BIANCHI	Institut Télécom/Télécom ParisTech/CNRS LTCI	Encadrant
Dr. Pablo PIANTANIDA	Supélec	Encadrant
Dr. Albin DUNAND	DGA IP/TSI/TTS	Invité
Prof. Jacques OKSMAN	Supélec	Invité (Directeur de thèse)

Remerciements / *Acknowledgments*

First of all, I would like to express my gratitude to my advisors Dr. Pascal Bianchi and Dr. Pablo Piantanida for their continuous trust, support, and guidance during all these years. I have really appreciated to work under their supervision in a both serious and friendly environment. I believe that their comments and advice will be useful my whole life and career. Furthermore, I would like to thank Dr. Pablo Piantanida for giving me the opportunity to meet Prof. Shlomo Shamai, who I have been very glad to work with, and wish to thank here for his helpful contributions and insights.

I am grateful to Prof. Giuseppe Caire and Prof. Vincent Poor for serving as my thesis reviewers, and to Dr. Pierre Duhamel, Dr. Olivier Rioul, and Prof. Mikael Skoglund for serving on the committee and attending the defense of this thesis.

I would like to thank Prof. Jacques Oksman for his advice, and the DGA (French Armement Procurement Agency) as well as its representative Dr. Albin Dunand for its support.

This experience would not have been so great without my workmates at Supélec and Télécom ParisTech. I would like to give a special thank to Jakob, Amr, Marina, Mari, Sheng and Marios at Supélec, and Sylvain(s), Alexandre, Amandine, Émilie(s), Sarah and Steffen at Télécom ParisTech.

Finally, my thoughts are with my girlfriend, family, and friends for their invaluable care and support.

Résumé

Cette thèse porte sur quelques problèmes de codage de source ciblé. Des résultats fondamentaux sont démontrés pour le codage de source dans les transmissions sécurisées (suivant l'approche de Shannon) et la quantification haute-résolution pour la détection (suivant l'approche de Bennett).

Les chapitres 2 et 3 portent sur la sécurité du point de vue de la théorie de l'information lors de la transmission d'une source via un canal, à débit limité ou bruité. Dans ce contexte, un capteur souhaite transmettre ses observations à une destination éloignée, en maintenant un adversaire (un espion, ou *eavesdropper*) aussi ignorant que possible. En utilisant les outils de la théorie de l'information introduits par Shannon (par ex. les séquences typiques ou le codage aléatoire), nous démontrons des résultats fondamentaux sur les performances des systèmes de codage. En particulier, nous démontrons des caractérisations symbole-par-symbole (*single-letter*) des régions débit-distorsion-incertitude correspondantes. Ces résultats sont appliqués à des scénarios classiques, par exemple pour des sources binaires ou gaussiennes.

Le chapitre 4 porte sur les règles de quantification pour la détection de processus stationnaires. Dans ce contexte, des capteurs souhaitent transmettre leurs observations à une destination éloignée qui effectue un test d'hypothèses (ou détection) à partir des données reçues. En utilisant les outils des théories de la quantification, de la détection et des processus stochastiques (par ex. le régime haute-résolution, les exposants d'erreur et les propriétés de mélangeance), nous démontrons des résultats fondamentaux sur les performances des quantificateurs dans un tel contexte. En particulier, nous démontrons une expression simple de la perte asymptotique en exposant d'erreur induite par la quantification. Celle-ci permet de déterminer des stratégies de quantification adaptées à la détection. Ces résultats sont illustrés dans quelques scénarios pratiques de détection.

Abstract

This thesis investigates some task-oriented source coding problems. Two different approaches are considered, following the frameworks of Shannon and Bennett, yielding fundamental results on source coding for secure transmission, and on high-rate quantization for detection, respectively.

Chapters 2 and 3 deal with information-theoretic security for the transmission of a source over a channel, either rate-limited or noisy. In such a setting, a sensor wants to transmit its observations to a remote destination while keeping an adversary (i.e., an eavesdropper) as ignorant as possible of this information. Using tools of Shannon information theory (e.g., typical sequences, random coding), we derive fundamental results on the performance of coding systems in several such contexts. Namely, we prove single-letter characterizations of the corresponding rate-distortion-equivocaiton region. These results are specialized in some standard scenarios e.g., for binary or Gaussian sources.

Chapter 4 deals with quantization rules for the detection of stationary processes. In such a setting, some sensors want to transmit their (correlated) observations to a remote destination that performs a binary hypothesis test on the received data. Using tools of quantization, detection, and stochastic processes theories (e.g., high-rate regime, error exponents, mixing properties, respectively), we derive fundamental results on the performance of quantizers in such a detection context. Namely, we prove a closed-form expression of the asymptotic loss in terms of error exponent due to quantization. As an application, we determine relevant detection-oriented quantization strategies. These results are applied to some practical detection scenarios.

Publications

Les travaux de cette thèse ont été publiés dans les articles suivants.
The material contained in this thesis appeared in the following publications.

Articles de revues / *Journal papers*

- J. Villard, P. Piantanida and S. Shamai
"Secure transmission of sources over noisy channels with side information at the receivers,"
soumis à *IEEE Transactions on Information Theory*, 2011.
- J. Villard and P. Piantanida
"Secure multiterminal source coding with side information at the eavesdropper,"
soumis à *IEEE Transactions on Information Theory*, Mai 2011.
- J. Villard and P. Bianchi
"High-rate vector quantization for the Neyman-Pearson detection of correlated processes,"
IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 5387–5409, 2011.

Conférences / *Conferences*

- J. Villard, P. Piantanida and S. Shamai
"Hybrid digital/analog schemes for secure transmission with side information,"
in *Proc. IEEE Information Theory Workshop* (ITW 2011),
Paraty, Brazil, October 16–20, 2011, pp. 678–682 (invité).
- J. Villard and P. Piantanida
"Codage de source sous contrainte de sécurité avec information adjacente aux récepteurs",
in *Actes du 23ème Colloque du GRETSI*,
Bordeaux, France, September 5-8, 2011.
- J. Villard and P. Bianchi
"Quantification vectorielle haute résolution pour la détection de processus stationnaires",
in *Actes du 23ème Colloque du GRETSI*,
Bordeaux, France, September 5-8, 2011.
- J. Villard, P. Piantanida and S. Shamai
"Secure lossy source-channel wiretapping with side information at the receiving terminals,"
in *Proc. IEEE International Symposium on Information Theory* (ISIT 2011),
Saint-Petersburg, Russia, July 31–August 5, 2011, pp. 1141–1145.

- J. Villard and P. Piantanida
  "Secure distributed lossless compression with side information at the eavesdropper,"
  in *Proc. 1st International ICST Workshop on Secure Wireless Networks* (Securenets 2011),
  Cachan, France, May 20, 2011 (invité).
- J. Villard and P. Piantanida
  "Secure lossy source coding with side information at the decoders,"
  in *Proc. 48th Annual Allerton Conference on Communication, Control, and Computing* (Allerton 2010),
  Allerton, IL, September 28–October 1, 2010, pp. 733–739.
- J. Villard and P. Bianchi
  "High-rate vector quantization for the Neyman-Pearson detection of some stationary mixing processes,"
  in *Proc. IEEE International Symposium on Information Theory* (ISIT 2010),
  Austin, TX, June 13–18, 2010, pp. 1608–1612.
- J. Villard, P. Bianchi, E. Moulines and P. Piantanida
  "High-rate quantization for the Neyman-Pearson detection of hidden Markov processes,"
  in *Proc. IEEE Information Theory Workshop* (ITW 2010),
  Cairo, Egypt, January 6–8, 2010, pp. 277–281.

Ces articles sont disponibles en prépublication sur arXiv[1] et à l'adresse suivante :
Electronic preprints are available on arXiv[1] *and at the following URL:*

http://www.joffrey-villard.fr/publications

[1] http://arxiv.org/a/villard_j_1

Plan général / *Outline*

Les principaux résultats de cette thèse sont présentés en français et en anglais, respectivement dans les parties I et II. Les détails complets apparaissent dans la partie II. À noter : la numérotation (des chapitres, sections, théorèmes, etc.) est identique dans les deux parties. Les annexes (rédigées en anglais et rassemblées dans la partie III) contiennent quelques rappels et les démonstrations secondaires.

The main results of this thesis are presented in both French and English in Parts I and II, respectively. Full details are provided in Part II. Note: The numbering (of chapters, sections, theorems, etc.) is identical in both parts. The appendices (gathered in Part III) provide some useful reminders as well as auxiliary proofs.

Première partie

Codage de source ciblé : Transmission sécurisée, Détection

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

BBAG	Bruit Blanc Additif Gaussien
CD	Centre de Décision
CDSM	Canal Discret Sans Mémoire
ECCE	État du Canal Connu à l'Émetteur
EQM	Erreur Quadratique Moyenne
i.i.d.	indépendants et identiquement distribués
LBG	Linde-Buzo-Gray
LRV	Logarithme du Rapport de Vraisemblance
NP	Neyman-Pearson
RCSF	Réseau de Capteur Sans Fil
TEB	Taux d'Erreur Binaire

CHAPITRE 1

Introduction

1.1 Préliminaires

La première transmission analogique de données sur ondes radio a été réalisée à la fin du XIX^{ème} siècle (et attribuée à Tesla, Marconi, et Popov, qui ont tous revendiqué l'invention de la *radio*), mettant en pratique la théorie des ondes électromagnétiques développée par Maxwell en 1865 pour transporter de l'information entre deux antennes. Au début du XX^{ème} siècle apparaissent les premières techniques numériques, comme la conversion analogique-numérique (réalisant l'échantillonnage et la quantification de signaux continus, en associant un symbole discret à une plage de valeurs), et la modulation numérique (permettant de transmettre une information numérique sur des signaux analogiques, en associant une forme d'onde à chaque symbole discret). Ces deux techniques fondamentales permettent la transmission de signaux analogiques dans un milieu de propagation (par ex. des ondes radio dans l'air) à travers une interface numérique, améliorant les performances en termes de fiabilité et d'utilisation des ressources [133]. La première technique numérique, appelée *pulse-code modulation* (PCM), a été brevetée par Reeves en 1938. Les domaines émergents du traitement du signal et du filtrage fournissaient alors les outils-clés pour la conception d'appareils performants.

Parallèlement, le développement de la théorie de la mesure [16], mené entre autres par Borel, Lebesgue, et Radon, a donné un nouvel élan aux probabilités et aux statistiques. Celle-ci fournit en effet les éléments de base pour l'axiomatisation de la théorie des probabilités de Kolmogorov [79]. De nombreux modèles de processus (chaînes de Markov, etc.) furent alors proposés, de même que les outils essentiels à leur analyse, comme la théorie ergodique qui concerne le comportement asymptotique (lorsque le temps croît à l'infini, par ex.) des systèmes dynamiques [159]. D'autre part, les statisticiens y ont trouvé les outils fondamentaux pour l'inférence statistique moderne, permettant le développement des théories de la détection [87] et de l'estimation [86].

D'une manière générale, l'inférence statistique a pour but de prendre une décision à propos d'un système à partir d'une expérience. Cette expérience produit des échantillons de données, et la décision concerne le modèle aléatoire sous-jacent. Par exemple, l'estimation de paramètre a pour but de trouver les valeurs des paramètres du modèle qui *expliquent* le mieux les données observées ; la détection a pour but de décider entre plusieurs possibilités (les *hypothèses*), par ex. détecter une cible dans une région sous surveillance avec des signaux radar [142].

En combinant la physique des ondes électromagnétiques et ces constructions ma-

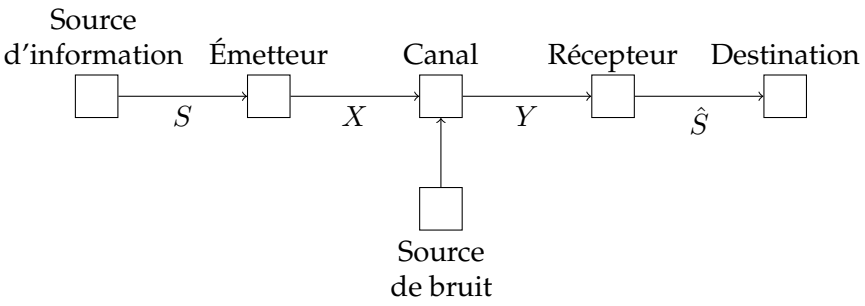


Figure 1.1 – Représentation schématique d'un système de communication [139].

thématiques, des modèles aléatoires de *sources* et de *canaux* ont été développés dans le contexte des télécommunications. Les composantes aléatoires de ces modèles traduisent le fait que les données transmises sont inconnues lors de la conception du système, que le milieu de propagation est complexe, variant dans le temps et inondé de rayonnements électromagnétiques (naturels ou provenant d'autres systèmes), et que les composants électroniques produisent du bruit thermique. En 1948, Shannon présenta sa *théorie mathématique des communications* [139], dans le but de proposer un modèle général pour le traitement et la transmission de l'information. Dans ce schéma, un système de communication (représenté à la figure 1.1) est composé

- d'une source d'information, qui produit des messages représentés par une variable aléatoire S à valeurs dans un ensemble $\mathcal{S}$,
- d'un émetteur, qui traite le message S et envoie un signal X dans le milieu de propagation,
- d'un canal $X \mapsto Y$, représenté par une probabilité de transition $p(y|x)$ (probabilité de recevoir y quand x est envoyé),
- d'un récepteur, qui calcule une reconstruction $\hat{S}$ du message S à partir du signal reçu Y,
- d'une destination, à laquelle le message est destiné.

Cette construction permet une analyse *théorique* de tout système de commmunication, fournissant de plus aux ingénieurs les limites fondamentales auxquelles comparer leurs méthodes pratiques.

Dans le cas de systèmes discrets, Shannon proposa d'utiliser l'*entropie* pour mesurer l'information (en fait, l'incertitude) des sources aléatoires. Pour une source S, cette entropie est définie par

$$H(S) = -\sum_{s\in\mathcal{S}} p(s)\log p(s)\ ,$$

où, pour tout $s \in \mathcal{S}$, $p(s)$ est la probabilité de l'événement $\{S = s\}$. Ses principaux résultats indiquent que les performances des systèmes de communication sont régies par des quantités de ce type. En particulier, Shannon démontra que la transmission d'une source

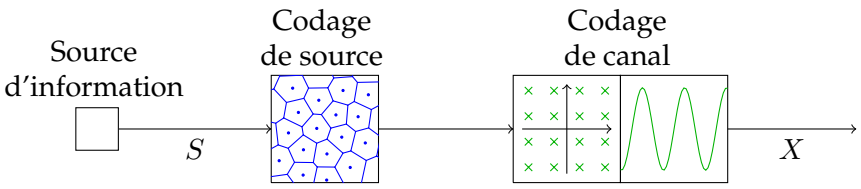


Figure 1.2 – Émetteur séparé.

S peut avoir lieu à un débit R si et seulement si son entropie $H(S)$ est inférieure à R. Si cette transmission est réalisée à travers un canal bruité $X \mapsto Y$, ce débit doit de plus être inférieur à la *capacité* du canal, définie par

$$C = \max_{p(x)} I(X;Y) \ ,$$

où $I(X;Y)$ est l'*information mutuelle* entre l'entrée et la sortie [31]. L'idée principale de la preuve est de permettre simultanément une petite proportion d'erreurs et de nombreuses transmissions. Ceci permet d'envoyer des redondances (voire des répétitions) qui vont aider à moyenner le bruit introduit par le canal et finalement identifier le message envoyé.

Les principaux outils pour l'analyse théorique d'un code (c'est-à-dire, les stratégies de transmission et de réception) sont le *codage aléatoire* et les *séquences typiques*, qui caractérisent les propriétés des séquences aléatoires lorsque leur longueur tend vers l'infini. Le résultat de base dans la démonstration de Shannon, appelé *propriété d'équipartition asymptotique*, a été étendu à une large classe de processus ergodiques (c'est le théorème de Shannon-McMillan-Breiman [21, 104]), généralisé par la suite de différentes façons [6, 51, 110]. Ces résultats ont ensuite permis de démontrer des théorème de codage plus généraux, par exemple pour des systèmes avec mémoire, ou des systèmes continus.

Les résultats de Shannon indiquent qu'il est *optimal* de séparer les étapes fondamentales réalisées à l'émission : tout d'abord compresser la source (*codage de source*), puis représenter les données compressées d'une manière adaptée au canal (*codage de canal*) – voir la figure 1.2. En d'autres termes, utiliser une interface numérique pour transmettre un signal analogique à travers un milieu de propagation (comme au tout début des communications numériques) est la meilleure stratégie.

Une attention considérable a été parallèlement portée au développement d'une *théorie de la quantification* pour les signaux continus (voir [53, 54]). En 1948, Oliver, Pierce et Shannon [118] ont analysé en profondeur la technique PCM et fourni une approximation de la distorsion *moyenne* introduite par un quantificateur uniforme lorsque le nombre de bits tend vers l'infini. Cette analyse à *haute résolution* a été par la suite étendue aux *companders* [8, 122]. Ces systèmes se composent d'un « compresseur » (une fonction inversible ϕ) suivi d'un quantificateur uniforme. La reconstruction finale est obtenue après « décompression », c'est-à-dire application du compresseur inversé ϕ^{-1} (voir la figure 1.3). En particulier, l'*intégrale de Bennett* [8, Eq. (1.6)] donne l'erreur quadratique moyenne (EQM) introduite par un *compander* transformant une source S en une reconstruction $\hat{S}_N$, lorsque

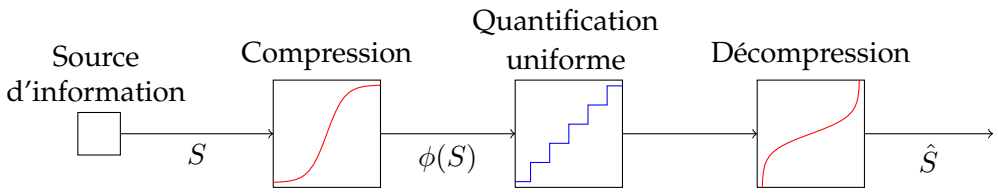


Figure 1.3 – Un *compander*.

le nombre N de niveaux de quantification tend vers l'infini :

$$\mathbb{E}\left[\left(\hat{S}_N - S\right)^2\right] \approx \frac{1}{12N^2} \int \frac{p(s)}{[\phi'(s)]^2}\,\mathrm{d}s\ .$$

Ce résultat a été généralisé aux quantificateurs à *densité*, ainsi qu'aux quantificateurs vectoriels (qui traitent les données par blocs) [111]. À partir de ces approximations asymptotiques, les chercheurs ont proposé des stratégies de quantification qui introduisent une faible distorsion moyenne pour divers modèles de source. Des algorithmes pour la réalisation pratique de ces stratégies ont également été développés [93, 99].

Notons que le but de cette approche est de concevoir de bons quantificateurs « autonomes », c'est-à-dire qui produisent une bonne estimée du message à la destination, en supposant une transmission fiable des données quantifiées, comme le permet le théomère de séparation [34, 139].

1.2 Systèmes pratiques

En accord avec ces résultats théoriques, et dans le but de faciliter les développements pratiques, les architectures par *couches* pour des systèmes *polyvalents* (comme celle représentée à la figure 1.4, et le modèle *Open Systems Interconnection* (OSI) [69]) sont rapidement devenues standard. Dans ces schémas, une tâche spécifique est assignée à chaque couche. En particulier, le codage de canal est réalisé dans la couche dite *physique* ; les couches supérieures supposent que l'information est alors sans erreur. L'idée générale est de disposer de blocs de base pouvant être conçus indépendamment. Les avancées dans un domaine (compression de données, correction d'erreurs, modulation, synchronisation, estimation de canal, contrôle d'accès) peuvent alors rapidement être implémentées et bénéficier à tous les sytèmes. De nombreuses technologies modernes de communication reposent sur de telles architectures par couches, comme le réseau internet (avec TCP/IP), ou le système téléphonique *Universal Mobile Telecommunications System* (UMTS).

Considérant que les ressources (l'information elle-même ou les machines qui la manipulent) peuvent être attaquées, le modèle OSI définit des services de *sécurité* [68]. Leur but est d'assurer les conditions *CID* (en anglais, *CIA triad*) :

- Confidentialité : L'information ne doit pas être révélée à des individus ou systèmes non autorisés ;

- Intégrité : Aucune modification ne doit être effectuée par un tiers sans être détectée ;
- Disponibilité : L'information doit être disponible à tout moment.

Ces services ne sont pas associés à une couche spécifique : chacune doit veiller à la sécurité de ses propres données. En pratique, la confidentialité est assurée par *chiffrement* complet [68], en utilisant des techniques de cryptographie essentiellement basées sur la complexité computationnelle. Notons que la sécurité repose alors seulement sur l'hypothèse que certaines opérations (par ex. la factorisation de grands entiers) ne peuvent être réalisées en pratique en temps raisonnable.

Au final, les appareils (émetteurs et récepteurs) de ces systèmes peuvent être modélisés par trois étages successifs (voir également la figure 1.4) :

- codage de source (ou compression de données),
- chiffrement des données,
- codage de canal.

Ces étages sont conçus séparément, indépendamment de l'utilisation finale des données traitées. Cependant, les résultats théoriques initiaux [139] sont valables pour les communications point-à-point, avec un émetteur qui souhaite envoyer à travers un canal une version compressée d'une source locale qui doit être précisément reconstruite à une destination, sans contrainte de sécurité (cf. figure 1.1). D'autres contextes peuvent se révéler beaucoup plus complexes. En particulier, de nombreux travaux ont été consacrés aux problèmes de compression à plusieurs terminaux [9, 143], de compression avec information adjacente [4, 155, 166], de détection [2, 153] et calcul [44, 108] distribués, de transmission sécurisée [32, 106, 165]. Nombre d'entre eux sont encore ouverts dans le cas général.

D'autre part, à mesure que les réseaux sans fil sont déployés à grande échelle, de nombreuses limitations apparaissent dans les technologies actuelles. Par exemple, le dé-

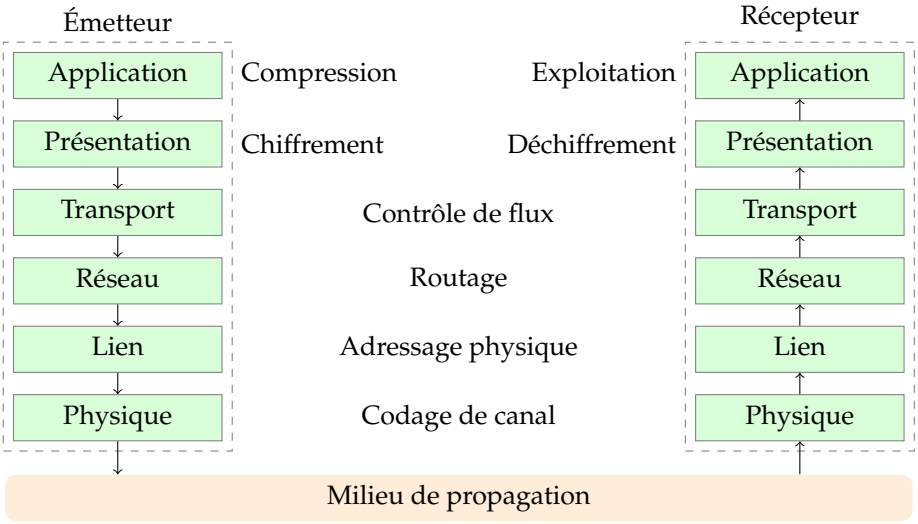


Figure 1.4 – Une architecture par couches et quelques tâches associées.

veloppement rapide de l'accès mobile à internet (avec par ex. la 3G) et des systèmes embarqués (dans les avions, les voitures, etc.) appelle à un bon usage des ressources (notamment du spectre de fréquences et de l'énergie) ; dans le cas contraire, les opérateurs pourraient rapidement faire face à de graves problèmes de congestion. De plus, de récentes avancées en électronique permettent de produire de petits appareils aux capacités limitées qui peuvent être déployés en masse pour former des réseaux de capteurs sans fil (RCSF) [5, 146]. En pratique, les RCSF peuvent être utiles pour gérer des lignes de production, détecter des événement anormaux et prévoir les catastrophes naturelles, surveiller une zone d'intérêt, détecter et localiser des cibles, etc. [88]. Les flottes de robots constituent également des exemples de systèmes de communication qui opèrent dans des environnements fortement contraints pour, par ex., l'exploration spatiale, l'extraction pétrolière ou les opérations de secours [22, 92]. Pour faire fonctionner de tels systèmes composés de nombreux agents, il semble nécessaire de développer des techniques efficaces *spécifiques* de mesure, de traitement de signal, de communication et de gestion de réseau.

1.3 Stratégies ciblées

Considérant que la destination ne souhaite pas tellement obtenir les données, mais les utiliser, les stratégies *ciblées* (ou *orientées*) constituent une tendance prometteuse pour les technologies sans fil émergentes et futures. En concevant des sytèmes pour une application particulière et en assouplissant la structure en couches (par ex., en permettant les optimisations inter-couches – *cross-layer*), elles visent à améliorer les performances pour certaines classes de problèmes. Par exemple, la gestion de la qualité de service devrait être différente selon que la destination souhaite télécharger un fichier en entier ou suivre une retransmission télévisée en direct. Des finalités différentes devraient amener des manières tout aussi différentes de mesurer la qualité, et plus généralement les performances. Estimant que l'utilisation finale des données devrait être la principale préoccupation des systèmes de communication, plusieurs concepts ont récemment émergé, comme les réseaux « centrés sur le contenu » [36], le routage [145] ou les architectures [67] « orientés application ».

En termes de codage de source, cette perspective a longtemps été considérée via la théorie *débit-distorsion* [10, 34, 141]. Dans ce contexte, la destination souhaite obtenir une approximation $\hat{S}^n$ de la séquence de source S^n à partir d'un message à débit limité ; la « qualité » de l'estimée finale est mesurée via la distorsion moyenne $\frac{1}{n}\sum_{i=1}^{n} d(S_i, \hat{S}_i)$, où $d\colon \mathcal{S} \times \mathcal{S} \to \mathbb{R}_+$ est une *mesure de distorsion*. Pour un débit donné, le but de l'émetteur est de trouver le schéma de codage qui minimise la distorsion induite. Il existe évidemment un compromis entre le débit et le niveau de distorsion autorisés, résumé par la fonction de *débit-distorsion* $R(D)$, définie comme le plus petit débit permettant une reconstruction avec un niveau de distortion d'au plus D. De toute évidence, d peut être adaptée à une application particulière. Par exemple, de nombreuses mesures « perceptuelles » ont été proposées pour la compression audio, de manière à quantifier la qualité

de la compression comme elle peut être ressentie par un utilisateur humain. Cependant, d'autres contextes sont difficiles à inclure dans la théorie débit-distorsion générale, principalement à cause de la structure du critère de distorsion ; celui-ci est la moyenne sur une séquence de distorsions mesurées symbole par symbole. De nouveaux résultats théoriques sont nécessaires dans ces cas-là.

Dans cette thèse, nous considèrons les problèmes suivants :

- codage de source pour les transmissions sécurisées, et
- codage de source pour la détection.

Les paragraphes ci-dessous donnent quelques préliminaires et un aperçu de nos contributions sur ces deux sujets. Dans les deux cas, une étude asymptotique permet d'obtenir une mesure déterministe des performances. L'optimisation de ces quantités donne les limites fondamentales des systèmes considérés en termes de performances, ainsi que des indications pour leur conception pratique.

1.3.1 Codage de source pour les transmissions sécurisées

Du fait que les ondes électromagnétiques se propagent librement, les communications sans fil sont particulièrement sensibles aux écoutes malveillantes. D'autre part, la nature aléatoire des sources d'information et des canaux de transmission peut être avantageusement utilisée pour fournir une sécurité supplémentaire. De manière à inclure de telles possibilités dans le cadre général des systèmes de communication [139], Shannon a défini la sécurité en termes d'information, dans laquelle le niveau de secret (la confidentialité) est mesuré via l'incertitude de l'espion – qui écoute la communication – à propos du message [140]. Cette approche repose uniquement sur les propriétés statistiques du système considéré. Elle assure donc une sécurité inconditionnelle, indépendamment des capacités (puissance de calcul, temps disponible, etc.) de l'espion. En particulier, les schémas de codage obtenus ne peuvent être cassés par force brute.

Depuis, les chercheurs ont étudié les communications sécurisées dans de nombreux contextes. La plupart des problèmes traditionnels ont été étendus pour inclure des contraintes de sécurité. En termes de codage de canal, Wyner a introduit le canal *wiretap* [165], où le canal de l'espion ($X \mapsto Z$) est une version dégradée de celui de l'utilisateur légitime ($X \mapsto Y$) (voir la figure 1.5), et a montré qu'il est possible de transmettre de l'information à un débit strictement positif avec une sécurité maximale jusqu'à la *secrecy capacity* C_s définie par

$$C_s = \max_{p(x)} I(X;Y|Z) \ .$$

Dans ce cas, l'espion ne peut obtenir aucune information à partir de la communication qu'il a écoutée. Le signal qu'il reçoit est en effet rendu quasi uniforme par l'ajout d'un bruit aléatoire numérique (introduit à l'émetteur) et par le canal, de sorte qu'il ne pourra jamais identifier le message envoyé [18].

Ce modèle a inspiré d'intenses recherches sur les aspects théoriques et pratiques de la sécurité au niveau de la couche physique [1,90,95], fournissant de nouveaux mécanismes

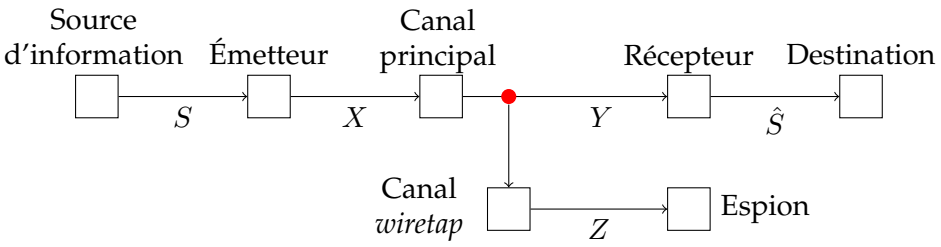


Figure 1.5 – Le canal *wiretap* [165].

non prévus dans le modèle OSI [68] pour sécuriser les communications. Alors que ces techniques introduisent des contraintes de sécurité au niveau du codage de canal, peu de résultats existent sur le codage de source sécurisé.

À la suite de la définition de la sécurité proposée par Shannon [140], l'incertitude de l'espion (à propos de la source) peut être utilisée en plus du niveau de distorsion au récepteur légitime pour mesurer les performances des stratégies de codage de source. Pour un débit donné, l'objectif de l'émetteur est alors de trouver le schéma de codage qui minimise la distorsion, tout en maximisant l'incertitude. Dans cette approche, les contraintes de sécurité sont directement prises en compte lors de la compression des données. Alors que le compromis à réaliser semble similaire, ce problème ne peut être inclus dans la théorie débit-distorsion classique : l'incertitude ne peut s'écrire comme une mesure de distorsion moyennée symbole par symbole. Une nouvelle dimension pour la sécurité doit donc être ajoutée au cadre de la théorie débit-distorsion.

Cette thèse (dans les chapitres 2 et 3) fournit des résultats fondamentaux sur le codage de source pour les *transmissions sécurisées*, en présence d'information adjacente aux récepteurs. Plus précisément, dans le chapitre 2, nous étudions le problème du *codage de source à plusieurs terminaux sous contrainte de sécurité*. Dans ce scénario, le système est composé de quatre noeuds :

- un émetteur principal (Alice), qui observe une source locale,
- un récepteur légitime (Bob), qui souhaite estimer la source d'Alice à partir de la version compressée qu'il reçoit via un lien (public) à débit limité,
- un second émetteur (Charlie), qui aide Bob à estimer la source d'Alice en envoyant une version compressée de sa propre observation (corrélée à la source d'Alice) via un lien (privé) à débit limité,
- un espion (Ève), qui observe parfaitement les bits transmis par Alice à Bob, et a également accès à une source, corrélée à celle d'Alice.

Par exemple, cette situation peut apparaître dans le contexte des RCSF : Alice et Charlie représentent alors des capteurs légitimes, Ève un capteur « piraté », et Bob un utilisateur distant qui souhaite être informé de l'environnement d'Alice en maintenant Ève aussi ignorante que possible. Dans ce contexte, Alice doit simultanément satisfaire les conditions sur le niveau de distorsion à Bob et l'incertitude à Ève. Des résultats fondamentaux

sur la région atteignable correspondante sont démontrés. En particulier, les schémas de codage *optimaux* sont caractérisés dans certains cas d'intérêt où les propriétés du système peuvent être pleinement exploitées pour la sécurité.

Dans le chapitre 3, les résultats du chapitre 2 sont partiellement étendus au cas de canaux bruités entre l'émetteur principal, Alice, et les récepteurs, Bob et Ève. Dans ce problème de *transmission sécurisée d'une source via un canal bruité, avec information adjacente aux récepteurs*, Charlie et Bob sont confondus, et Alice a toujours pour objectif de satisfaire simultanément les contraintes de distorsion et de sécurité, tirant profit des caractéristiques des sources et des canaux. A priori, les schémas du chapitre 2 combinés avec ceux pour le canal *wiretap* [32,165] peuvent être utiles mais ne sont pas nécessairement optimaux. Cette thèse fournit des résultats fondamentaux sur la *région débit-distorsion-incertitude*. Dans ce contexte, de nouveaux schémas numériques et hybrides analogiques/numériques sont proposés.

1.3.2 Codage de source pour la détection

Dans un problème de détection, un utilisateur souhaite identifier une situation (parmi plusieurs possibilités, appelées *hypothèses*), à partir de l'observation d'un certain signal. Dans le cas de deux hypothèses, $\mathsf{H0}$ (dans un contexte de radar, la région sous surveillance est dégagée) et $\mathsf{H1}$ (une cible est présente), il y a deux manières de prendre une décision erronée. Soit l'utilisateur décide que les échantillons observés proviennent de la distribution correspondant à l'hypothèse $\mathsf{H1}$ alors que la vraie est $\mathsf{H0}$ (*fausse alarme*), soit il décide $\mathsf{H0}$ au lieu de $\mathsf{H1}$ (*manque*). Les probabilités de ces deux événements, respectivement notées α et β, caractérisent les performances du détecteur (ou test). Ces deux grandeurs ne peuvent être maximisées simultanément ; il faut réaliser un compromis. Celui-ci peut être visualisé via la courbe ROC (pour *receiver operating characteristic*), qui représente $1-\beta$ en fonction de α [76]. Sous certaines hypothèses, cette courbe ROC converge vers la constante 1 (qui correspond à un détecteur parfait) à une vitesse exponentielle, lorsque le nombre n d'échantillons observés tend vers l'infini :

$$\beta \simeq \exp(-n\,K),$$

où K est le taux de convergence, indépendant de α, et appelé *exposant d'erreur*. Cette quantité est une mesure-clé pour concevoir des tests avec de bonnes performance pratiques (pour un n fini).

Si l'utilisateur est loin du phénomène d'intérêt, il peut recevoir les données d'un capteur distant. Ces deux entités forment alors un système de communication comme celui de la figure 1.1. Pour un débit donné, l'objectif de l'émetteur est ici de trouver le schéma de codage qui maximise l'exposant d'erreur. Si les échantillons sont indépendants et identiquement distribués (i.i.d.) sous chacune des hypothèses, ce dernier correspond à la divergence de Kullback-Leibler entre les distributions sous $\mathsf{H0}$ et $\mathsf{H1}$ [81]. Cependant, la théorie débit-distorsion classique ne s'applique pas : l'exposant d'erreur ne peut pas s'écrire comme une mesure de distorsion traditionnelle.

Cette thèse (dans le chapitre 4) étudie quelques aspects théoriques de la quantification pour la détection. En supposant que la source peut être modélisée par un processus multivarié stationnaire ergodique, nous suivons l'approche de [61, 111] pour analyser l'impact de la quantification sur les performances du test de Neyman-Pearson. Notre principale contribution est de fournir une expression compacte de l'exposant d'erreur correspondant dans le régime des *hautes résolutions*, c.-à-d. lorsque le nombre de niveaux de quantification tend vers l'infini. Ce résultat peut être vu comme l'équivalent de l'intégrale de Bennett [8] dans le contexte de la détection d'un processus corrélé multivarié. Il est valable sous certaines conditions de mélangeance du processus observé, ainsi que certaines hypothèses sur le comportement asymptotique des quantificateurs dans le régime des hautes résolutions. À partir de cette expression, des stratégies de quantification adaptées à la détection sont déterminées.

CHAPITRE 2

Codage de source à plusieurs terminaux sous contrainte de sécurité

Résumé. Ce chapitre traite du problème de codage de source à plusieurs terminaux sous contrainte de sécurité, lorsque l'adversaire dispose d'une information adjacente. Dans ce scénario, un encodeur souhaite compresser une source en satisfaisant à la fois des contraintes de distortion (pour un récepteur légitime) et d'incertitude (pour un récepteur adverse). On suppose qu'un lien à débit limité relie l'encodeur aux deux récepteurs. Le récepteur légitime est de plus aidé par un second encodeur qui envoie une version compressée de sa propre source (corrélée à la première) via un lien privé à débit limité. L'adversaire a également accès à une troisième source corrélée qu'il peut utiliser comme information adjacente. Ce contexte peut par exemple être vu comme l'unification entre le problème de Berger-Tung et celui de la compression sous contrainte de sécurité. Des bornes intérieure et extérieure à la région débit-distorsion-incertitude, optimales dans certains cas, sont proposées. Les différences statistiques entre les informations aux récepteurs et une distorsion non nulle peuvent être parfaitement exploitées en termes de sécurité. Des sources gaussiennes et binaires sont étudiées à titre d'exemples.

2.1 Introduction

Considérons le problème classique consistant à compresser une source (observée par un capteur, Alice) pour qu'elle puisse être estimée avec un niveau de distorsion fixé à une certaine destination (Bob), un lien public à débit limité étant disponible entre les deux appareils. Ce lien est supposé parfaitement accessible à un adversaire (Ève), par exemple un capteur corrompu, qui dispose également de sa propre observation corrélée à la source. Lors de la communication, l'encodeur souhaite dévoiler aussi peu que possible sa source à l'adversaire. Un autre capteur (Charlie) peut aider Bob à estimer la source d'Alice en envoyant une version compressée de sa propre observation (corrélée à la source) via un lien privé à débit limité, uniquement observé par Bob. Dans ce contexte, la corrélation entre les observations peut être utile, non seulement pour diminuer les débits de transmission, mais aussi pour augmenter la sécurité du système, définie ici par l'incertitude de Ève à propos de la source d'Alice. D'un point de vue théorique, le problème considéré ici est très riche et toujours non résolu, dans la mesure où il contient, comme sous-problèmes, celui de la compression distribuée avec perte, ouvert de longue date, ainsi que celui du codage de source avec contrainte de sécurité, plus récemment étudié.

Slepian et Wolf [143] ont introduit le problème de compression distribuée sans perte, où Bob souhaite estimer parfaitement les sources d'Alice et Charlie. Wyner [163] et Ahlswede et Körner [4] ont par la suite caractérisé la région atteignable lorsqu'une seule source doit être estimée (codage de source avec information adjacente partielle). La généralisation du contexte de Slepian-Wolf à des niveaux de distorsion arbitraires pour chaque source a été introduit par Berger [9]. Ce dernier a de plus fourni des bornes intérieure et extérieure à la région atteignable correspondante, distinctes dans le cas général. De nombreux résultats d'optimalité ont été démontrés dans les cas d'information adjacente non codée [166], de recontruction parfaite d'au moins une source [12], et dans certains cas particuliers, dont celui des sources gaussiennes avec mesure de distorsion quadratique [119, 158]. Dans les dernières décennies, ces sujets ont été l'objet d'intenses recherches, et des progrès remarquables ont été réalisés des points de vue théorique et pratique. Ceux-ci incluent la définition d'un cadre général pour la compression sans perte avec de multiples terminaux [33, 63], le codage de source avec perte en présence d'information adjacente incertaine au récepteur [66, 73], la compression avec perte pour des encodeurs partiellement séparés [72] ou plusieurs décodeurs [150–152], des résultats d'optimalité pour des sources gaussiennes dans divers contextes [134, 148], ainsi que la conception de codes imbriqués pour la compression distribuée en utilisant par ex., les codes par contrôle de parité [174], par réseaux [98, 138, 174], ou par treillis algébriques [132]. Malgré ces avancées, le simple problème de la compression distribuée avec perte, introduit par Berger [9], est toujours ouvert.

D'autre part, la problématique des communications sécurisées a généré de très nombreux travaux. L'attention s'est particulèrement portée sur la cryptographie traditionnelle, basée sur la complexité computationnelle. Dans cette approche, la sécurité repose uniquement sur l'hypothèse que certains problèmes ne peuvent être résolus en pratique en temps raisonnable. En 1949, Shannon [140] a défini une notion de la sécurité en termes d'information, dans laquelle le niveau de secret est mesuré via l'incertitude de l'espion à propos du message. Cette approche permet de considérer les problématiques de sécurité au niveau de la couche physique, et assure une sécurité inconditionnelle, indépendamment des capacités de l'espion. Utilisant cette notion dans une perspective de codage de canal, Wyner a introduit le canal *wiretap* [165] et montré qu'il est possible de transmettre de l'information avec une sécurité maximale dès lors que le canal de l'espion est une version dégradée de celui de l'utilisateur légitime. Csiszàr et Körner [32] ont étendu ce résultat au cas général des canaux de diffusion avec une incertitude arbitraire. Depuis, de nombreuses extensions ont été proposées [1, 90, 95], par ex. pour les canaux à évanouissement [89], de même que des schémas de codage pratiques pour les communications sécurisées, par ex. des codes imbriqués pour les canaux *wiretap* de type-II [96] et la construction de codes spécifiques pour la sécurité à partir de codes ordinaires [65]. Cependant, peu de travaux existent en ce qui concerne le codage de source avec contrainte de sécurité, alors qu'il a été démontré que la présence de corrélation entre différentes observations permet de garantir une certaine sécurité [3, 103].

On peut identifier deux approches dans la littérature sur le codage de source sous

contrainte de sécurité. Il est en effet supposé soit qu'un lien sécurisé à débit limité est déjà disponible entre Alice et Bob (permettant l'utilisation de clés secrètes), soit que les récepteurs ont accès à quelque information adjacente à propos de la source. Dans le cas du partage de clés secrètes, les compressions sans et avec perte ont été étudiées dans de nombreux contextes [105, 169–172]. Lorsque les récepteurs n'ont aucune information adjacente, il est montré que la stratégie optimale consiste à appliquer le codage de source avec perte classique, suivi du chiffrement en utilisant la clé secrète [172]. Dans le deuxième cas, des travaux récents [131] ont considéré le codage de source sans perte avec information adjacente (non codée) à chacun des récepteurs, en supposant un lien à débit non limité entre Alice et Bob. Dans ce contexte, il est démontré que le schéma de Slepian-Wolf classique est insuffisant. Le codage de source sans perte avec information adjacente codée (respectivement la compression sans perte distribuée) a été étudiée récemment [56, 147] (resp. [55]). Dans leur scénario *"one-sided helper"*, les auteurs de [147] ont caractérisé la région atteignable lorsqu'une seule source doit être parfaitement estimée et Ève n'a pas d'information adjacente. En particulier, il est démontré que le schéma de Wyner [163] et Ahlswede-Körner [4] permet d'atteindre la région toute entière. Des bornes intérieures et extérieures à la région atteignable pour la compression sans perte distribuée ont également été proposées [55]. Le codage de source *avec perte* sous contrainte de sécurité, avec information adjacente aux récepteurs a reçu moins d'attention. En particulier, si les informations adjacentes sont dégradées, la région atteignable peut être obtenue à partir des résultats de [106] et le schéma de Wyner-Ziv [166] est optimal.

Dans ce chapitre, nous étudions le problème général du codage de source avec perte pour des sources sans mémoire, avec information adjacente codée au récepteur légitime, en présence d'un espion qui observe à la fois les bits transmis et une source corrélée (voir la figure 2.1). Les liens entre émetteurs et récepteurs sont supposés sans bruit, de sorte qu'ils ne peuvent fournir aucun avantage en termes de sécurité. Ce problème peut être vu comme l'extension de celui de Berger et al. [11] avec des contraintes de sécurité. Nous donnons des bornes intérieure et extérieure à la région atteignable, appelée *région débit-distorsion-incertitude*. Ces bornes sont disjointes dans le cas général, en raison d'une condition de Markov particulière, comme dans [9, 11]. À partir de la région intérieure proposée, nous démontrons deux résultats d'optimalité dans les cas (*i*) d'information adjacente non codée aux récepteurs, généralisant les résultats de [56, 131] à un niveau de distorsion arbitraire, et (*ii*) de la reconstruction sans perte des deux sources au récepteur légitime (compression sans perte distribuée), améliorant les résultats de [55]. Dans le cas du codage avec perte en présence d'information adjacente non codée, si l'une des informations adjacentes (celle de Bob ou de Ève) est moins bruitée que l'autre, alors le schéma de Wyner-Ziv est suffisant. De même, pour la compression sans perte distribuée, il est montré que si l'information adjacente de Ève est moins bruitée que l'observation de Charlie, alors le schéma de Slepian-Wolf permet d'atteindre la région toute entière. Un exemple d'application est fourni dans le cas du codage de source avec perte d'une source gaussienne, étendant les résultats d'Oohama [119] pour prendre en compte les contraintes de sécurité. Nous considérons également le cas du codage de source avec

perte d'une source binaire, où l'information adjacente (non codée) à Bob (resp. Ève) est produite à partir de la source via un canal binaire à effacement (resp. un canal binaire symétrique).

La suite de ce chapitre est organisée de la manière suivante. La section 2.2 donne les définitions pour le codage de source securisé avec perte, en présence d'information adjacente codée au récepteur légitime. Les principaux résultats, c.-à-d. les bornes intérieure et extérieure à la région débit-distorsion-incertitude, y sont également énoncés. La preuve de la borne intérieure est donnée à la section 2.3. La section 2.4 (resp. 2.5) fournit une caractérisation optimale de la région atteignable dans le cas d'information adjacente non codée à Bob (resp. compression sans perte distribuée). La section 2.6 est dédiée aux exemples d'application pour des sources gaussiennes et binaires. La section 2.7 conclut le chapitre.

Notations

Pour toute suite $(x_i)_{i\in\mathbb{N}^*}$, x_k^n désigne la collection $(x_k, x_{k+1}, \ldots, x_n)$. x_1^n est simplement noté x^n. Soit $\mathcal{T}$ un ensemble fini arbitraire. Le cardinal de $\mathcal{T}$ est noté $\|\mathcal{T}\|$. Pour tout sous-ensemble $\mathcal{S} \subseteq \mathcal{T}$, $\mathbf{1}_{\mathcal{S}}$ désigne la fonction indicatrice de $\mathcal{S}$ dans $\mathcal{T}$: pour tout $t \in \mathcal{T}$, $\mathbf{1}_{\mathcal{S}}(t) = 1$ si $t \in \mathcal{S}$, et $\mathbf{1}_{\mathcal{S}}(t) = 0$ sinon. L'entropie est notée $H(\cdot)$, et l'information mutuelle $I(\cdot;\cdot)$. On désigne les ensembles typiques et conditionnellement typiques par $T_\delta^n(X)$ et $T_\delta^n(Y|x^n)$, respectivement (voir l'annexe A). Soient X, Y et Z trois variables aléatoires de distribution p. Si $p(x|yz) = p(x|y)$ pour tous x, y, z, alors elles forment une chaîne de Markov, notée $X \multimap Y \multimap Z$. La variable aléatoire Y est dite moins bruitée que Z par rapport à X si $I(U;Y) \geq I(U;Z)$ pour toute variable aléatoire U telle que $U \multimap X \multimap (Y, Z)$ forment une chaîne de Markov. Cette relation est notée $Y \succeq_X Z$. L'ensemble des nombres réels positifs est noté $\mathbb{R}_+$. Pour tout $x \in \mathbb{R}$, $[x]_+$ désigne $\max\{0\,;x\}$. Les logarithmes sont pris en base 2 et notés $\log(\cdot)$. L'entropie binaire est définie sur $[0\,;1]$ par $h_2(x) = -x\log(x) - (1-x)\log(1-x)$. Son inverse h_2^{-1} est définie sur $[0\,;1]$ et à valeurs dans $[0\,;\frac{1}{2}]$. Pour tous $a, b \in [0\,;1]$, $a \star b = a(1-b) + (1-a)b$.

2.2 Codage de source avec perte sous contrainte de sécurité, avec information adjacente codée

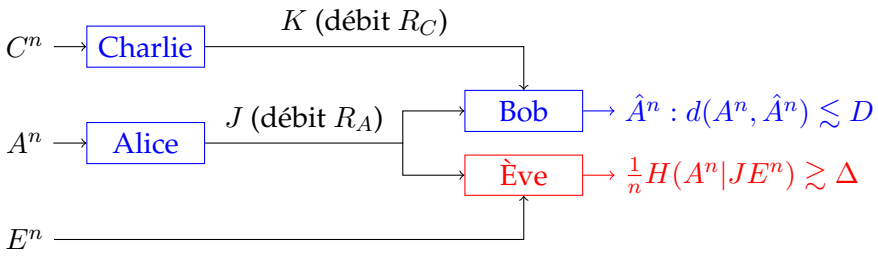


Figure 2.1 – Codage de source avec perte sous contrainte de sécurité, avec information adjacente codée.

2.2.1 Définitions

Dans cette section, nous formalisons le contexte représenté à la figure 2.1. Soient $\mathcal{A}$, $\mathcal{C}$ et $\mathcal{E}$ trois ensembles finis. Alice, Charlie et Ève observent les suites de variables aléatoires $(A_i)_{i\in\mathbb{N}^*}$, $(C_i)_{i\in\mathbb{N}^*}$ et $(E_i)_{i\in\mathbb{N}^*}$, respectivement, à valeurs dans $\mathcal{A}$, $\mathcal{C}$ et $\mathcal{E}$, resp. Pour tout $i \in \mathbb{N}^*$, les variables aléatoires A_i, C_i et E_i sont distribuées selon la loi $p(ace)$ sur $\mathcal{A}\times\mathcal{C}\times\mathcal{E}$. De plus, elles sont indépendantes au cours du temps.

Soit $d\colon \mathcal{A}\times\mathcal{A} \to [0\,;d_{\max}]$ une mesure de distorsion finie, c.-à-d. telle que $0 \leq d_{\max} < \infty$. On note également d la distorsion moyenne des composantes sur $\mathcal{A}^n \times \mathcal{A}^n$: pour tous $a^n, b^n \in \mathcal{A}^n$, $d(a^n, b^n) \triangleq \frac{1}{n}\sum_{i=1}^n d(a_i, b_i)$.

Définition 2.1 (Code)**.** Un code (n, R_A, R_C) pour le codage de source est défini par

- une fonction d'encodage à Alice $f_A\colon \mathcal{A}^n \to \{1,\dots,2^{nR_A}\}$,
- une fonction d'encodage à Charlie $f_C\colon \mathcal{C}^n \to \{1,\dots,2^{nR_C}\}$,
- une fonction de décodage à Bob $g\colon \{1,\dots,2^{nR_A}\}\times\{1,\dots,2^{nR_C}\} \to \mathcal{A}^n$.

Définition 2.2 (Atteignabilité)**.** Un quadruplet $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ est dit *atteignable* si, pour tout $\varepsilon > 0$, il existe un code $(n, R_A+\varepsilon, R_C+\varepsilon)$, (f_A, f_C, g), tel que :

$$\mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] \leq D + \varepsilon\,,$$
$$\frac{1}{n} H(A^n|f_A(A^n), E^n) \geq \Delta - \varepsilon\,.$$

L'ensemble des quadruplets atteignables est noté $\mathcal{R}^*$ et appelé *région débits-distorsion-incertitude*.

Remarque 2.1. La région $\mathcal{R}^*$ est fermée et convexe.

Remarque 2.2. Les quantités apparaissant dans la définition 2.2 dépendent uniquement des distributions marginales $p(ac)$ et $p(ae)$. Il en est de même pour les résultats ci-dessous, qui fournissent des bornes intérieure et extérieure à la région $\mathcal{R}^*$.

2.2.2 Borne intérieure

Le théorème suivant donne une borne intérieure à la région $\mathcal{R}^*$: il définit la région $\mathcal{R}_{\text{int}} \subseteq \mathcal{R}^*$. La démonstration est basée sur un codage par superposition et du *random binning* à Alice et Charlie, et sur un décodage conjoint à Bob. L'incertitude à Ève peut être caractérisée via les propriétés des séquences typiques.

Théorème 2.1 (Borne intérieure). *Un quadruplet $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ est atteignable s'il existe des variables aléatoires U, V, W sur des ensembles finis $\mathcal{U}, \mathcal{V}, \mathcal{W}$, resp., telles que $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$R_A \geq I(V;A|W)\,, \tag{2.1}$$

$$R_C \geq I(W;C|V)\,, \tag{2.2}$$

$$R_A + R_C \geq I(VW;AC)\,, \tag{2.3}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V,W))\big]\,, \tag{2.4}$$

$$\Delta \leq H(A|VW) + I(A;W|U) - I(A;E|U)\,, \tag{2.5}$$

$$\Delta - R_C \leq H(A|V) - I(A;E|U) - I(W;C|V)\,. \tag{2.6}$$

La région $\mathcal{R}_{int}$ est définie comme l'enveloppe convexe de l'ensemble de ces quadruplets.

Démonstration. Voir la section 2.3. □

La région intérieure ci-dessus est également atteignable par une combinaison de trois familles complémentaires de codes. Cette approche est présentée à la page 39 (voir l'*Esquisse de la preuve*).

Les inégalités (2.1)–(2.3) sont identiques à celles de Berger-Tung [9]. Elles assurent la parfaite reconstruction des variables V et W par Bob, qui peut alors calculer l'estimée

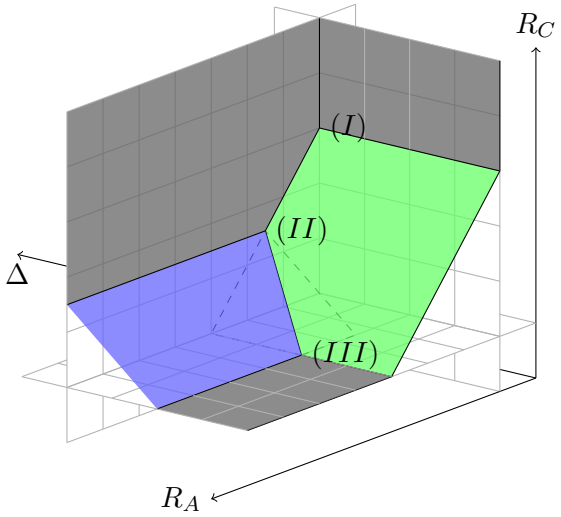


Figure 2.2 – Triplets (R_A, R_C, Δ) atteignables pour un niveau de distorsion D fixé.

$\hat{A}(V,W)$ de A. La contrainte sur la somme des débits (2.3) traduit le compromis entre R_A et R_C : l'information doit être transmise par l'un ou l'autre des émetteurs.

Donnons à présent quelques indications sur (2.5) et (2.6). Le premier terme $H(A|VW)$ correspond à l'incertitude de Bob. Alice exploite donc la distorsion admissible à Bob pour augmenter l'incertitude à Ève. De plus, pour des variables V et W données (déterminant les débits et le niveau de distorsion) la variable auxiliaire U peut être ajustée pour rendre Bob « meilleur » que Ève, en maximisant $I(A;W|U)-I(A;E|U)$. Cette quantité représente le gain (ou la perte) de Ève en termes d'incertitude. Dans le même temps, (2.6) impose un compromis entre l'incertitude à Ève Δ et le débit de Charlie R_C. Cette inégalité traduit le fait que Δ ne peut être grande si R_C ne l'est pas : si la contrainte de sécurité est forte, plus d'information doit être envoyé via le lien privé (entre Charlie et Bob). Nous appellerons cette quantité $\Delta - R_C$ le *débit secret public*.

Notons que (2.5) s'écrit également

$$\Delta \leq H(A|UE) - I(V;A|UW)\ .$$

La variable U est donc considérée comme un *message commun*, comme si Ève pouvait la décoder. En fait, en cas d'information adjacente à Bob non codée (resp. de compression sans perte distribuée), la proposition 2.8 (resp. 2.13) montre qu'il est optimal d'encoder U de sorte que Ève puisse parfaitement l'estimer. Le reste de l'information envoyée via le lien public, $I(V;A|UW)$, est directement soustrait de l'incertitude, indiquant qu'il est traité comme des bits « bruts » de A.

Esquisse de la preuve du théorème 2.1 (approche par combinaison). En premier lieu, nous construisons trois codes qui atteignent les points (I), (II) et (III) illustrés sur les figures 2.2, 2.3 et 2.4. Chaque point est atteint en utilisant un schéma de communication en trois étapes, dont le but est de transmettre les variables (U,V) et W, descriptions de A à Alice et de C à Charlie, respectivement, à Bob. Notons de plus que le codage par *superposition* impose que V soit « au-dessus » de U, et donc décodé après. À chaque étape, l'information précédemment reçue (et décodée) est utilisée comme information adjacente à Bob. Comme dans le codage de Wyner-Ziv [166], on effectue un *random binning* pour utiliser au mieux cette information adjacente. Les trois schémas correspondent à toutes les combinaisons de l'ensemble $\{U,V,W\}$ telles que U est avant V, comme indiqué par la ligne 2

Point	(I)	(II)	(III)
Ordre décod.	W, U, V	U, W, V	U, V, W
R_A	$I(V;A\|W)$	$I(U;A)+I(V;A\|UW)$	$I(V;A)$
R_C	$I(W;C)$	$I(W;C\|U)$	$I(W;C\|V)$
D	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$
Δ	$H(A\|UE)-I(V;A\|UW)$	$H(A\|UE)-I(V;A\|UW)$	$H(A\|UE)-I(V;A\|U)$

Tableau 2.1 – Les trois points atteignables.

du tableau 2.1. Pour chaque schéma, l'incertitude à Ève peut être caractérisée en suivant le raisonnement donné à la section 2.3.3. Après exécution de l'algorithme d'élimination de Fourier-Motzkin [156], on peut démontrer que les trois schémas proposés atteignent les points (I), (II) et (III), dont les coordonnées sont données dans le tableau 2.1.

Les points (I) et (II) correspondent à des niveaux de distorsion D et d'incertitude Δ identiques (voir la figure 2.4). Par une combinaison des schémas correspondants (*time-sharing*), chaque point du segment (I)–(II) est également atteignable, avec une distorsion D et une incertitude Δ. Ce segment peut être facilement décrit du fait que la quantité $R_A + R_C$ est identique pour les deux points (I) et (II) (voir la figure 2.3).

Les points (II) et (III) correspondent à un niveau de distorsion identique D. Par une combinaison des schémas correspondants, chaque point du segment (II)–(III) est également atteignable, avec une distorsion D. Ce segment peut être facilement décrit : les quantités $R_A + R_C$ et $\Delta - R_C$ sont identiques pour les deux points (II) et (III) (voir les figures 2.3 et 2.4, resp.).

Les segments (I)–(II) et (II)–(III) décrivent ensemble une région délimitée par six hyperplans, donnés par les équations du théorème 2.1. □

Remarque 2.3. La projection des points (I) et (III) sur le plan $\Delta = 0$ (correspondant au cas où il n'y a pas de contrainte de sécurité) sont ceux obtenus par Berger-Tung [9]. Dans ce cas, le point (II) est inutile : il est atteignable par une simple combinaison des points (I) and (III) (voir la figure 2.3). Dans le cas général, le schéma proposé peut cependant augmenter la sécurité de la transmission, comme le montre la figure 2.4.

Remarque 2.4. Lorsqu'il n'y a aucune contrainte de sécurité, Jana et Blahut [70] ont récemment démontré l'équivalence des bornes intérieures de [9] et [11], indiquant que le point (I) seul peut décrire la même région que les points (I) et (III) (après prise de l'enveloppe convexe). Un tel résultat dans notre contexte avec contrainte de sécurité ne semble pas évident.

Remarque 2.5. L'union simple des régions données par les équations du théorème 2.1 n'est pas convexe. En effet, une variable T de partage du temps (*time-sharing*) ne peut être

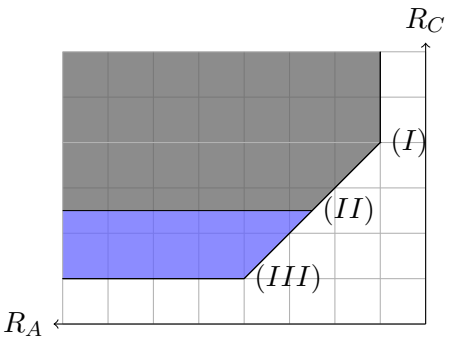


Figure 2.3 – Projection sur le plan $\Delta = 0$.

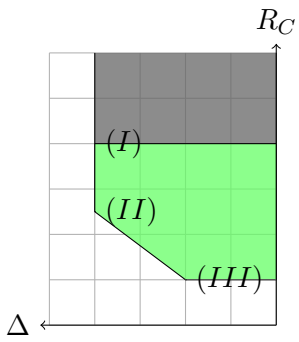


Figure 2.4 – Projection sur le plan $R_A = 0$.

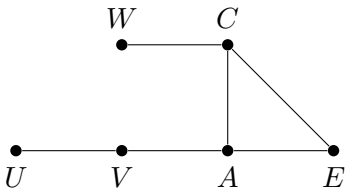


Figure 2.5 – Borne intérieure – Représentation graphique de la distribution $p(uvwace)$.

ajoutée aux variables auxiliaires U, V et W. Cela casserait la longue chaîne de Markov $U \multimap V \multimap A \multimap C \multimap W$, essentielle dans notre schéma de codage (voir également la figure 2.5, et l'annexe B pour une description de ce type de représentations graphiques).

La proposition suivante permet de majorer les cardinaux des alphabets $\mathcal{U}$, $\mathcal{V}$ et $\mathcal{W}$. La preuve est basée sur le théorème de Fenchel-Eggleston-Carathéodory et suit le raisonnement classique (voir [42, Appendix C]).

Proposition 2.2 (Cardinaux)**.** *Dans la caractérisation de la région $\mathcal{R}_{int}$ donnée par le théorème 2.1, il suffit de considérer des ensembles $\mathcal{U}$, $\mathcal{V}$ et $\mathcal{W}$ tels que $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 5$, $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 5)(\|\mathcal{A}\| + 3)$, et $\|\mathcal{W}\| \leq \|\mathcal{C}\| + 3$.*

Démonstration. Voir l'annexe D.3. □

2.2.3 Borne extérieure

Le théorème suivant donne une borne extérieure à la région $\mathcal{R}^*$: il définit $\mathcal{R}_{\text{ext}} \supseteq \mathcal{R}^*$.

Théorème 2.3 (Borne extérieure)**.** *La région $\mathcal{R}^*$ est un sous-ensemble de $\mathcal{R}_{ext}$, défini comme la fermeture de l'ensemble des quadruplets $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ tels qu'il existe des variables aléatoires U, V, W sur des ensembles finis $\mathcal{U}, \mathcal{V}, \mathcal{W}$, respectivement, de lois $p(wace) = p(w|c)p(ace)$, $p(uvace) = p(u|v)p(v|a)p(ace)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$\begin{aligned} R_A &\geq I(V;A|W)\ , \\ R_C &\geq I(W;C|V)\ , \\ R_A + R_C &\geq I(VW;AC)\ , \\ D &\geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\ , \\ \Delta &\leq H(A|VW) + I(A;W|U) - I(A;E|U)\ , \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V)\ . \end{aligned}$$

Démonstration. Voir l'annexe D.4. □

De même que dans le problème classique de codage de source à plusieurs terminaux [9], la région extérieure ressemble à la région intérieure. Elle est cependant convexe sans *time-sharing*, et les conditions de Markov $W \multimap C \multimap (A,E)$ et $U \multimap V \multimap A \multimap (C,E)$ sont plus faibles que la longue chaîne du théorème 2.1 (comparer les figures 2.5 et 2.6).

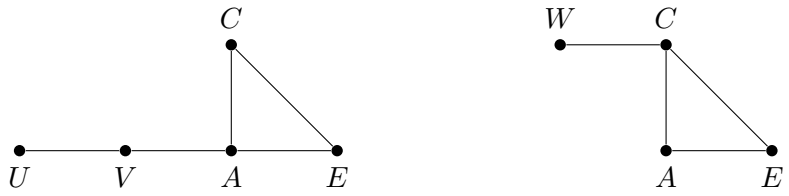


Figure 2.6 – Borne extérieure – Représentations graphiques de $p(uvace)$ et $p(wace)$.

2.3 Démonstration du théorème 2.1 (Borne intérieure)

Soient trois variables aléatoires U, V, W sur les ensembles finis $\mathcal{U}, \mathcal{V}, \mathcal{W}$, respectivement, de loi jointe $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$, une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, et un quadruplet $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$. Nous décrivons dans cette section un schéma qui atteint (sous certaines conditions) le quadruplet (R_A, R_C, D, Δ) : pour tout $\varepsilon > 0$, nous construisons un code $(n, R_A + \varepsilon, R_C + \varepsilon)$, (f_A, f_C, g), tel que

$$\mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] \leq D + \varepsilon\,,$$
$$\frac{1}{n} H(A^n | f_A(A^n), E^n) \geq \Delta - \varepsilon\,.$$

Soient $\varepsilon > 0$, $R_1, R_2 \in \mathbb{R}_+^*$ tels que $R_1 + R_2 = R_A + \varepsilon$, et $S_1 \geq R_1$, $S_2 \geq R_2$, $S_C \geq R_C + \varepsilon$. Dans les paragraphes suivants, nous exposons les principes de la stratégie de codage utilisée. Les détails sont donnés dans la section 2.3 de la partie II.

2.3.1 Encodage à Alice et Charlie

Alice compresse A en U, puis en V, via deux dictionnaire de séquences typiques u^n et v^n. Pour tirer parti de l'information adjacente à Bob, elle sépare aléatoirement (à chaque étape) ces mots de code en plusieurs groupes (*random binning*), comme dans le codage de Wyner-Ziv [166] (voir la figure 2.7). D'après les propriétés des séquences typiques, on peut montrer que la probabilité que cette procédure échoue tend vers zéro quand n tend vers l'infini, si $S_1 > I(U;A)$ et $S_2 > I(V;A|U)$.

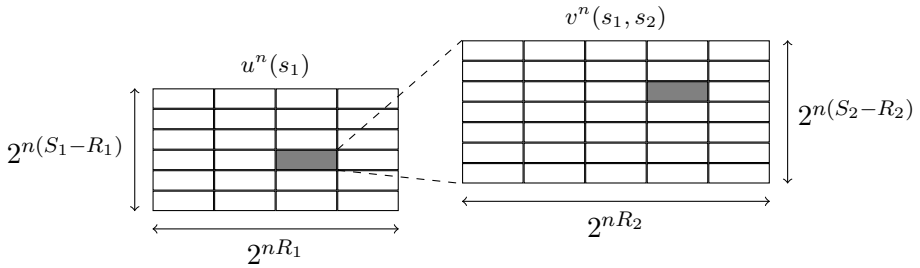


Figure 2.7 – Dictionnaire d'Alice.

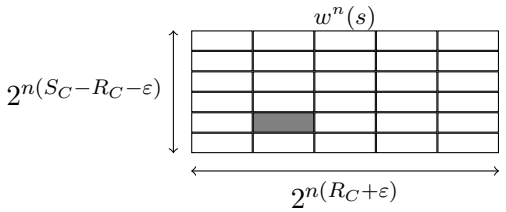


Figure 2.8 – Dictionnaire de Charlie.

Charlie compresse C en W, via un dictionnaire de séquences typiques w^n, et sépare aléatoirement ces mots de code en plusieurs groupes (voir la figure 2.8). La probabilité d'erreur de cette procédure est négligeable pour n suffisamment grand si $S_C > I(W;C)$.

Ces deux procédures d'encodage produisent les messages $J = f_A(A^n) \triangleq (r_1, r_2) \in \{1, \dots, 2^{nR_1}\} \times \{1, \dots, 2^{nR_2}\}$ à Alice, et $K = f_C(C^n) \triangleq r_C \in \{1, \dots, 2^{n(R_C+\varepsilon)}\}$ à Charlie. Ceux-ci sont transmis à Bob via les liens sans erreur correspondants.

2.3.2 Décodage à Bob

À partir des trois indices reçus (r_1, r_2, r_C), Bob décode les variables U, V et W en cherchant l'unique triplet (u^n, v^n, w^n) de mots de code *conjointement* typiques dont les numéros de groupes sont (r_1, r_2, r). On peut montrer que ce décodage échoue avec une faible probabilité si les conditions suivantes sont vérifiées :

$$\begin{aligned} S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon &< I(V;W)\ , \\ S_1 - R_1 + S_2 - R_2 &< I(V;W)\ , \\ S_2 - R_2 &< I(V;W|U)\ . \end{aligned}$$

Bob calcule alors l'estimée $g(J,K) \in \mathcal{A}^n$ à partir de la relation suivante :

$$g_i(J,K) \triangleq \hat{A}(v_i, w_i)\ , \quad \text{pour tout } i = \{1, \dots, n\}\ .$$

La distorsion moyenne de cette estimée peut être facilement caractérisée. Pour n assez grand, elle vérifie l'inégalité suivante :

$$\mathbb{E}\Big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\Big] \leq \mathbb{E}\big[d(A, \hat{A}(V,W))\big] + \varepsilon\ .$$

La condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V,W))\big]$ est donc suffisante pour atteindre un niveau de distorsion $D + \varepsilon$ à Bob.

2.3.3 Incertitude à Ève

L'incertitude à Ève (moyennée sur l'ensemble des dictionnaires possibles) peut être bornée inférieurement de la manière suivante :

$$\begin{aligned}\frac{1}{n}H(A^n|f_A(A^n),E^n) &= \frac{1}{n}H(A^n|r_1r_2E^n)\\ &= \frac{1}{n}\Big[H(A^n|r_1E^n) - I(A^n;r_2|r_1E^n)\Big]\\ &\geq H(A|UE) - R_2 - \varepsilon\,,\end{aligned}$$

La condition $\Delta \leq H(A|UE) - R_2$ est donc suffisante pour atteindre une incertitude $\Delta - \varepsilon$.

2.3.4 Fin de la démonstration

Les équations suivantes fournissent des conditions suffisantes pour l'atteignabilité du quadruplet (R_A, R_C, D, Δ) : pour tout $\varepsilon > 0$,

$$\begin{cases} R_1 > 0\\ R_2 > 0\\ R_A + \varepsilon = R_1 + R_2\\ R_C \geq 0\\ S_1 \geq R_1\\ S_2 \geq R_2\\ S_C \geq R_C + \varepsilon\\ S_1 > I(U;A)\\ S_2 > I(V;A|U)\\ S_C > I(W;C)\\ S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V;W)\\ S_1 - R_1 + S_2 - R_2 < I(V,W)\\ S_2 - R_2 < I(V;W|U)\\ D \geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\\ \Delta \leq H(A|UE) - R_2 \end{cases}$$

L'algorithme d'élimination de Fourier-Motzkin [156] conduit au système suivant.

$$\begin{cases} R_A + \varepsilon > I(V;A|W)\\ R_C + \varepsilon > I(W;C|V)\\ R_A + R_C + 2\varepsilon > I(VW;AC)\\ D \geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\\ \Delta < H(A|VW) + I(A;W|U) - I(A;E|U)\\ \Delta - R_C - \varepsilon < H(A|V) - I(A;E|U) - I(W;C|V) \end{cases}$$

□

2.4 Codage de source avec perte sous contrainte de sécurité, avec information adjacente non codée

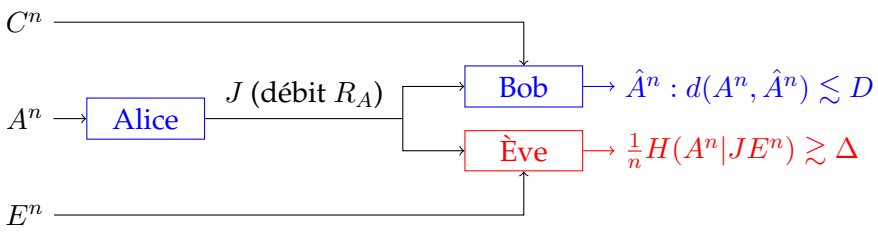


Figure 2.9 – Codage de source avec perte sous contrainte de sécurité, avec information adjacente non codée.

2.4.1 Définitions

Dans cette section, nous considèrons le cas particulier représenté à la figure 2.9 où Bob a accès à une information adjacente *non codée* (Bob et Charlie sont confondus).

Définition 2.3 (Code)**.** Un code (n, R_A) pour le codage de source dans ce contexte est défini par

- une fonction d'encodage à Alice $f\colon \mathcal{A}^n \to \{1, \dots, 2^{nR_A}\}$,
- une fonction de décodage à Bob $g\colon \{1, \dots, 2^{nR_A}\} \times \mathcal{C}^n \to \mathcal{A}^n$.

Définition 2.4 (Atteignabilité)**.** Un triplet $(R_A, D, \Delta) \in \mathbb{R}_+^3$ est dit *atteignable* si, pour tout $\varepsilon > 0$, il existe un code $(n, R_A + \varepsilon)$, (f, g), tel que :

$$\mathbb{E}\left[d\big(A^n, g(f(A^n), C^n)\big)\right] \leq D + \varepsilon \,,$$
$$\frac{1}{n} H(A^n|f(A^n), E^n) \geq \Delta - \varepsilon \,.$$

L'ensemble des triplets atteignables est noté $\mathcal{R}_{\text{nc}}^*$ et appelé *région débit-distorsion-incertitude*.

2.4.2 Caractérisation optimale

Le théorème suivant donne une caractérisation symbole-par-symbole (*single-letter*) de la région $\mathcal{R}_{\text{nc}}^*$.

Théorème 2.6 (Caractérisation de $\mathcal{R}_{\text{nc}}^*$)**.** *La région $\mathcal{R}_{nc}^*$ est égale à la fermeture de l'ensemble des triplets $(R_A, D, \Delta) \in \mathbb{R}_+^3$ tels qu'il existe des variables aléatoires U, V sur des ensembles finis $\mathcal{U}$, $\mathcal{V}$, resp., de loi jointe $p(uvace) = p(u|v)p(v|a)p(ace)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, vérifiant les inégalités suivantes:*

$$R_A \geq I(V; A|C) \,, \tag{2.7}$$
$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, C))\big] \,, \tag{2.8}$$
$$\Delta \leq H(A|VC) + I(A; C|U) - I(A; E|U) \,. \tag{2.9}$$

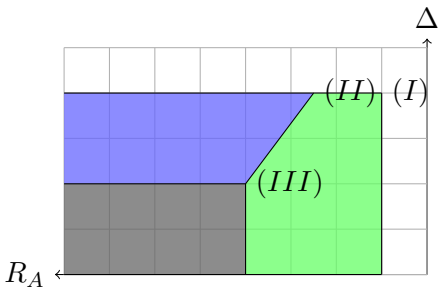


Figure 2.10 – Projection sur le plan $R_C = 0$.

Démonstration. L'atteignabilité est une conséquence du théorème 2.1, en choisissant $W = C$, et en supprimant les contraintes sur R_C (c.-à-d. en faisant tendre R_C vers $+\infty$). Autrement dit, la région ci-dessus est celle décrite par le point (I) (voir la figure 2.10).

Une nouvelle démonstration est nécessaire pour la réciproque (voir l'annexe D.5). □

Les commentaires de la section 2.2.2 à propos du théorème 2.1 sont également valables ici : (2.7) et (2.8) sont classiques dans la théorie débit-distorsion ; Alice peut exploiter la distorsion admissible à Bob pour augmenter l'incertitude à Ève (cf. le terme $H(A|VC)$ dans (2.9)) ; et la variable auxiliaire U peut être ajustée pour maximiser la quantité $I(A;C|U) - I(A;E|U)$.

La proposition suivante permet de majorer les cardinaux des alphabets $\mathcal{U}$, $\mathcal{V}$.

Proposition 2.7 (Cardinaux)**.** *Dans la caractérisation de la région $\mathcal{R}_{nc}^*$ donnée par le théorème 2.6, il suffit de considérer des ensembles $\mathcal{U}$ et $\mathcal{V}$ tels que $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 2$, and $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$.*

Démonstration. La preuve est similaire à celle de la proposition 2.2 (donnée en annexe D.3). Les détails sont omis. □

2.4.3 Caractérisation alternative

La proposition suivante peut être démontrée à partir du théorème 2.6.

Proposition 2.8 (Caractérisation alternative)**.** *La région $\mathcal{R}_{nc}^*$ est égale à la fermeture de l'ensemble des triplets $(R_A, D, \Delta) \in \mathbb{R}_+^3$ tels qu'il existe des variables aléatoires U, V sur des ensembles finis $\mathcal{U}$, $\mathcal{V}$, resp., de loi jointe $p(uvace) = p(u|v)p(v|a)p(ace)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$R_A \geq \Big[I(U;C) - I(U;E)\Big]_+ + I(V;A|C)\,, \tag{2.10}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\,, \tag{2.11}$$

$$\Delta \leq H(A|VC) + I(A;C|U) - I(A;E|U)\,. \tag{2.12}$$

Démonstration. Les inégalités (2.10)–(2.12) décrivent une région plus petite que (2.7)–(2.9). L'atteignabilité de la proposition ci-dessus est donc une conséquence du théorème 2.6.

Notons que le membre de droite de (2.9) et (2.12) s'écrit

$$H(A|VC) + I(A;C) - I(A;E) - \Big[I(U;C) - I(U;E)\Big] .$$

Maximiser cette somme par rapport à U revient à minimiser $I(U;C) - I(U;E)$. Dans le pire des cas, choisir $U = \emptyset$ annule ce terme. Cela indique que le choix optimal U^* donne toujours $I(U^*;C) - I(U^*;E) \leq 0$, et rend (2.7) et (2.10) identiques. □

La proposition 2.8 et la démonstration ci-dessus indiquent que le choix optimal de U est une variable aléatoire U^* qui peut être décodée par Ève. Cependant, comme minimiser la quantité $I(U;C) - I(U;E)$ par rapport à U correspond à chercher une sous-partie de V qui contient plus d'information à propos de E que de C, ce *message commun* donne peu d'information à Ève.

2.4.4 Cas particuliers

2.4.4.1 Codage sans perte

Le corollaire suivant est une conséquence du théorème 2.6.

Corollaire 2.9. *En cas de reconstruction sans perte de A à Bob, la région $\mathcal{R}^*_{nc}$ est égale à la fermeture de l'ensemble des triplets $(R_A, D = 0, \Delta) \in \mathbb{R}^3_+$ tels qu'il existe une variable aléatoire U sur un ensemble fini $\mathcal{U}$, t.q. $U \multimap A \multimap (C, E)$ forment une chaîne de Markov et*

$$\begin{aligned} R_A &\geq H(A|C) , \\ \Delta &\leq I(A;C|U) - I(A;E|U) . \end{aligned}$$

2.4.4.2 Information adjacente de Bob moins bruitée ($C \succeq_A E$)

Corollaire 2.10. *Si l'information adjacente de Bob est* moins bruitée *que celle de Ève, alors la région $\mathcal{R}^*_{nc}$ est égale à la fermeture de l'ensemble des triplets $(R_A, D, \Delta) \in \mathbb{R}^3_+$ tels qu'il existe une variable aléatoire V sur un ensemble fini $\mathcal{V}$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$ telles que $V \multimap A \multimap (C, E)$ forment une chaîne de Markov et*

$$\begin{aligned} R_A &\geq I(V;A|C) , \\ D &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big] , \\ \Delta &\leq H(A|VC) + I(A;C) - I(A;E) . \end{aligned}$$

Dans ce cas, la variable auxiliaire U du théorème 2.6 est constante, et le schéma de Wyner-Ziv [166] permet d'atteindre la région toute entière.

2.4.4.3 Information adjacente de Ève moins bruitée ($E \succeq_A C$)

Corollaire 2.11. *Si l'information adjacente de Ève est* moins bruitée *que celle de Bob, alors la région $\mathcal{R}^*_{nc}$ est égale à la fermeture de l'ensemble des triplets $(R_A, D, \Delta) \in \mathbb{R}^3_+$ tels qu'il existe une variable aléatoire V sur un ensemble fini $\mathcal{V}$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$ telles que $V \multimap A \multimap (C, E)$ forment une chaîne de Markov et*

$$\begin{aligned} R_A &\geq I(V;A|C)\ , \\ D &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\ , \\ \Delta &\leq H(A|VE)\ . \end{aligned}$$

Dans ce cas, la variable auxiliaire U du théorème 2.6 est choisie égale à V et le schéma de Wyner-Ziv [166] permet d'atteindre la région toute entière. L'incertitude à Ève correspond au cas où celle-ci peut décoder V. Ici, Alice peut seulement exploiter la distorsion admissible à Bob pour atteindre une incertitude non nulle à Ève.

2.5 Compression sans perte distribuée sous contrainte de sécurité

2.5.1 Définitions

Dans cette section, nous considérons le cas où Bob souhaite parfaitement reconstruire les deux source A et C, à partir des messages J et K (voir la figure 2.11).

Définition 2.5 (Code)**.** Un code (n, R_A, R_C) pour la compression distribuée dans ce contexte est défini par

- une fonction d'encodage à Alice $f_A\colon \mathcal{A}^n \to \{1, \dots, 2^{nR_A}\}$,
- une fonction d'encodage à Charlie $f_C\colon \mathcal{C}^n \to \{1, \dots, 2^{nR_C}\}$,
- une fonction de décodage à Bob $g\colon \{1, \dots, 2^{nR_A}\} \times \{1, \dots, 2^{nR_C}\} \to \mathcal{A}^n \times \mathcal{C}^n$.

Définition 2.6 (Atteignabilité)**.** Un triplet $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ est dit *atteignable* si, pour tout $\varepsilon > 0$, il existe un code $(n, R_A + \varepsilon, R_C + \varepsilon)$, (f_A, f_C, g), tel que :

$$\begin{aligned} \Pr\left\{g(f_A(A^n), f_C(C^n)) \neq (A^n, C^n)\right\} &\leq \varepsilon\ , \\ \frac{1}{n} H(A^n | f_A(A^n), E^n) &\geq \Delta - \varepsilon\ . \end{aligned}$$

L'ensemble des triplets atteignables est noté $\mathcal{R}^*_{\text{sp}}$.

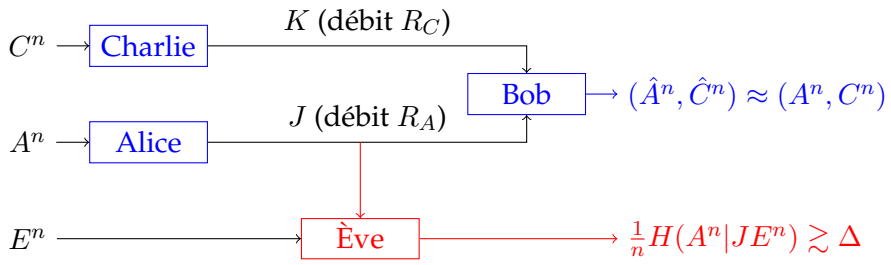


Figure 2.11 – Compression sans perte distribuée avec contrainte de sécurité.

2.5.2 Caractérisation optimale

Le théorème suivant donne une caractérisation symbole-par-symbole (*single-letter*) de la région $\mathcal{R}^*_{\text{sp}}$.

Théorème 2.12 (Caractérisation de $\mathcal{R}^*_{\text{sp}}$)**.** *La région $\mathcal{R}^*_{sp}$ est égale à la fermeture de l'ensemble des triplets $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ tels qu'il existe une variable aléatoire U sur un ensemble fini $\mathcal{U}$ vérifiant la chaîne de Markov $U \multimap A \multimap (C, E)$ et les inégalités suivantes :*

$$R_A \geq H(A|C) \,, \tag{2.13}$$

$$R_C \geq H(C|U) \,, \tag{2.14}$$

$$R_A + R_C \geq H(AC) \,, \tag{2.15}$$

$$\Delta \leq I(A; C|U) - I(A; E|U) \,. \tag{2.16}$$

Démonstration. L'atteignabilité vient de celle des points (I) et (II), en prenant $V = A$ et $W = C$ (voir la section 2.2.2).

Une nouvelle démonstration est nécessaire pour la réciproque. Celle-ci est donnée en annexe D.6. □

Les inégalités (2.13)–(2.15) ressemblent à celles de Slepian et Wolf [143, Section III]. Elles assurent une reconstruction parfaite des variables A et C à Bob. En fonction de la distribution de (A, C, E), la variable U peut être ajustée pour atteindre une incertitude non nulle à Eve (cf. (2.16)). Si l'information adjacente de Ève E est *moins bruitée* que C ($E \succeq_A C$), alors choisir $U = A$ est optimal, et le schéma de Slepian-Wolf permet d'atteindre la région toute entière (avec $\Delta = 0$).

En cas d'information adjacente non codée à Bob, le théorème 2.12 donne directement le corollaire 2.9 en faisant tendre R_C vers l'infini.

2.5.3 Caractérisation alternative

De même que dans la section 2.4 pour le codage de source avec perte et information adjacente non codée, nous pouvons démontrer ici une caractérisation alternative de la région $\mathcal{R}^*_{\text{sp}}$.

Proposition 2.13 (Caractérisation alternative)**.** *La région $\mathcal{R}^*_{sp}$ est égale à la fermeture de l'ensemble des triplets $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ tels qu'il existe une variable aléatoire U sur un ensemble $\mathcal{U}$ vérifiant la chaîne de Markov $U \multimap A \multimap (C, E)$ et les inégalités suivantes :*

$$R_A \geq \big[I(U;C) - I(U;E)\big]_+ + H(A|C)\,, \tag{2.17}$$

$$R_C \geq H(C|U)\,, \tag{2.18}$$

$$R_A + R_C \geq H(AC)\,, \tag{2.19}$$

$$\Delta \leq I(A;C|U) - I(A;E|U)\,. \tag{2.20}$$

Démonstration. L'atteignabilité est une conséquence du théorème 2.12.

Une nouvelle démonstration est nécessaire pour la réciproque (voir l'annexe D.7). □

Cette nouvelle caractérisation indique que « donner U à Ève est optimal ». Le débit supplémentaire $[I(U;C) - I(U;E)]_+$ ne change pas l'incertitude à Ève. Ce résultat est à mettre en parallèle avec ceux sur le canal *wiretap* [32, 90], où un *message commun* est transmis de sorte à pouvoir être décodé par Ève, sans changer la région atteignable.

2.6 Exemples d'application

2.6.1 Sources gaussiennes avec information adjacente codée

Considérons le modèle de source représenté à la figure 2.12 où la source d'Alice est une variable normale centrée réduite, et les observations de Charlie et Ève sont les sorties de canaux indépendants à bruit blanc additif gaussien (BBAG) avec A en entrée, de gains ρ_C, ρ_E, et de puissance de bruit $(1-\rho_C^2)$, $(1-\rho_E^2)$, resp., avec $0 < \rho_C, \rho_E < 1$.

Bien que le théorème 2.1 soit énoncé pour des sources sur alphabets finis, nous prenons la liberté de considérer qu'il fournit également une région atteignable pour les sources gaussiennes, avec une mesure de distorsion appropriée (la distance euclidienne sur $\mathbb{R}$, $d(a,b) = (a-b)^2$, pour tous $a, b \in \mathbb{R}$), en utilisant l'*entropie différentielle* $h(\cdot)$, et en considérant des incertitudes $\Delta \in \mathbb{R}$. La *région débits-distorsion-incertitude* est ici notée $\mathcal{R}^*_{\mathrm{G}}$.

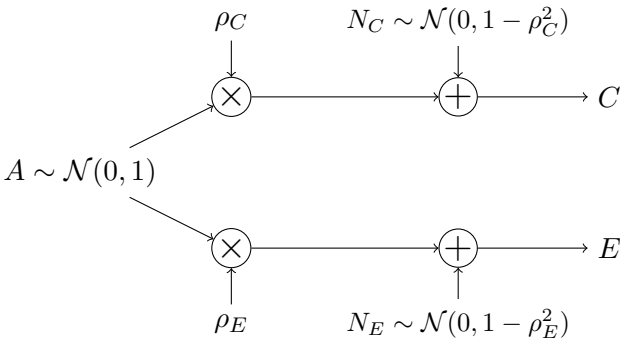


Figure 2.12 – Sources gaussiennes.

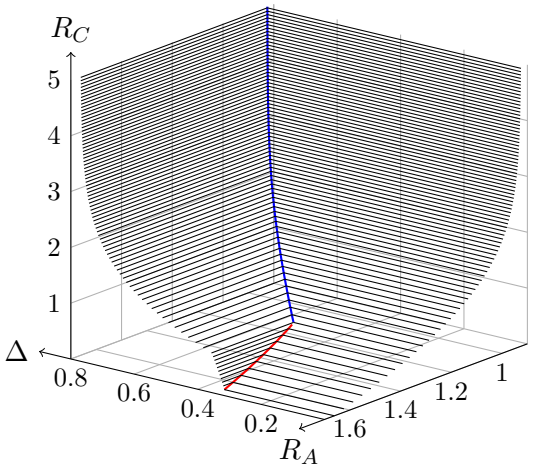


Figure 2.13 – Triplets (R_A, R_C, Δ) atteignables dans le cas gaussien quadratique ($\rho_C = 0.8$, $\rho_E = 0.6$, $D = 0.1$).

Remarque 2.6. Dans ce contexte gaussien, une incertitude atteignable Δ donne un minorant $2^{2\Delta}/(2\pi e)$ de l'erreur quadratique moyenne de tout estimateur de A à Ève (voir par ex. [31, Theorem 8.6.6]).

La proposition 2.14 ci-dessous donne une borne intérieure à $\mathcal{R}_{\mathrm{G}}^*$ basée sur l'atteignabilité du point (I) (voir la section 2.2.2). Ce choix est motivé par [119, Theorem 1] où Oohama démontre que ce point est optimal lorsqu'une seule source doit être estimée avec un certain niveau de distorsion (sans contrainte de sécurité). La figure 2.13 représente cette région intérieure pour $\rho_C = 0.8$, $\rho_E = 0.6$ et $D = 0.1$.

Proposition 2.14 (Borne intérieure). *Un quadruplet* $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$ *est atteignable si :*

$$
\begin{aligned}
R_A &\geq \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ , \\
\Delta &\leq \frac{1}{2}\log\left(2\pi e(1-\rho_E^2)\right) \\
&\qquad -\frac{1}{2}\min\left\{\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ ; \right. \\
&\qquad\qquad \left. \log\left(1+(1-\rho_E^2)\left[\frac{1}{D}-\frac{1}{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}\right]_+\right)\right\} .
\end{aligned}
$$

Démonstration. Voir l'annexe D.8. □

Si Ève n'a pas d'information adjacente, c.-à-d. si $\rho_E = 0$, alors la région intérieure donnée par la proposition 2.14, et correspondant au schéma de Oohama [119], est optimale.

Proposition 2.15 (Caractérisation optimale). *Si $\rho_E = 0$, alors la région $\mathcal{R}_G^*$ est égale à l'ensemble des quadruplets $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$ tels que :*

$$R_A \geq \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ ,$$
$$\Delta \leq \frac{1}{2}\log(2\pi e) - \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ .$$

Démonstration. L'atteignabilité est une conséquence de la proposition 2.14. La réciproque se démontre en suivant le raisonnement de [119] (voir l'annexe D.9). □

Remarque 2.7. En cas d'information adjacente non codée à Bob, c.-à-d. si $R_C \to \infty$, la région intérieure donnée par la proposition 2.14 est optimale si $\rho_C \geq \rho_E$, c.-à-d. si $C \succeq_A E$. Nous conjecturons que ce résultat est également valable si $\rho_C < \rho_E$, bien que la démonstration semble plus complexe.

2.6.2 Source binaire avec informations adjacentes CBE/CBS

Considérons le modèle de source représenté à la figure 2.14, où la source est binaire, uniformément distribuée, et l'information adjacente de Bob (resp. Ève) est produite à partir de A via un canal binaire à effacement (CBE) de probabilité d'effacement $\beta \in [0\,;1]$ (resp. un canal binaire symétrique (CBS) de probabilité d'erreur $\epsilon \in [0\,;\frac{1}{2}]$). La distance de Hamming est utilisée comme mesure de distorsion à Bob d.

Ce modèle possède un intérêt particulier, car ni Bob ni Ève n'est un décodeur moins bruité pour tous (β, ϵ). En effet, en fonction des valeurs des paramètres (β, ϵ), on peut montrer [113] que le canal de diffusion $A \mapsto (C, E)$ possède les propriétés suivantes :

(*a*) Si $0 \leq \beta \leq 2\epsilon$, E est une version stochastiquement dégradée de C ;

(*b*) Si $2\epsilon \leq \beta \leq 4\epsilon(1-\epsilon)$, C est moins bruitée que E ($C \succeq_A E$) ;

(*c*) Si $4\epsilon(1-\epsilon) \leq \beta \leq h_2(\epsilon)$, C est « meilleure » que E ($I(A;C) \geq I(A;E)$) ;

(*d*) Si $h_2(\epsilon) < \beta \leq 1$, aucune des relations ci-dessus n'est valable entre C et E.

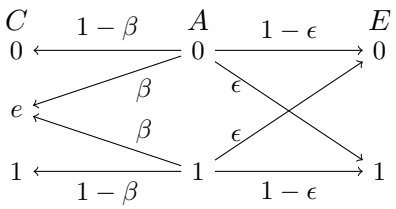


Figure 2.14 – Source binaire avec informations adjacentes CBE/CBS.

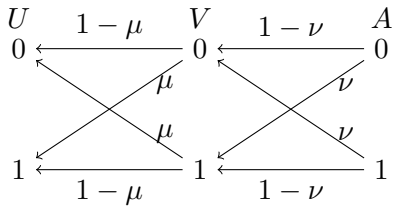


Figure 2.15 – Variables auxiliaires binaires.

Le corollaire 2.10 donne donc une caractérisation optimale de la région $\mathcal{R}_{\text{nc}}^*$ lorsque β vérifie la condition (*a*) ou (*b*). Dans les autres cas, seul le théorème 2.6 s'applique, et la variable U n'est ni constante ni égale à V.

D'après la proposition 2.7, nous savons qu'il suffit de considérer des ensembles $\mathcal{U}$ et $\mathcal{V}$ tels que $\|\mathcal{U}\| \leq 4$ et $\|\mathcal{V}\| \leq 12$. En fait, la proposition suivante indique que nous pouvons restreindre notre attention à des variables auxiliaires (U, V) obtenues en sortie d'un canal de diffusion binaire symétrique dégradé avec A en entrée (voir la figure 2.15). Notons que V est identique à la variable auxiliare de Wyner et Ziv [166] pour la fonction débit-distorsion d'une source binaire, lorsqu'il n'y a pas d'espion.

Proposition 2.16 (Caractérisation optimale)**.** *La région $\mathcal{R}_{nc}^*$ est égale à l'ensemble des triplets $(R_A, D, \Delta) \in \mathbb{R}_+^3$ tels qu'il existe $\nu, \mu \in [0\,;\frac{1}{2}]$ vérifiant les inégalités suivantes :*

$$\begin{aligned} R_A &\geq \beta\,(1 - h_2(\nu))\,, \\ D &\geq \beta\,\nu\,, \\ \Delta &\leq \beta\,h_2(\nu) + (1-\beta)\,h_2(\nu \star \mu) - h_2(\epsilon \star \nu \star \mu) + h_2(\epsilon)\,. \end{aligned}$$

Démonstration. L'atteignabilité est une application directe du théorème 2.6, en définissant les variables U et V comme indiqué par la figure 2.15, et la fonction $\hat{A}$ sur $\mathcal{V} \times \mathcal{C} = \{0,1\} \times \{0, e, 1\}$ par

$$\hat{A}(v,c) = \begin{cases} c & \text{si } c \neq e \\ v & \text{sinon} \end{cases}$$

La démonstration de la réciproque est donnée en annexe D.10. □

Remarque 2.8. Un niveau de distorsion atteignable D est un majorant du taux d'erreur binaire (TEB) à Bob (lorsqu'il estime A) :

$$\mathbb{E}\big[d(A^n, g(f(A^n), C^n))\big] = \frac{1}{n}\sum_{i=1}^{n} \Pr\left\{\hat{A}_i \neq A_i\right\}\,,$$

où $\hat{A}_i \triangleq g_i(f_A(A^n), C^n)$ est la $i^{\text{ème}}$ composante de l'estimée de A^n à Bob. D'autre part, une incertitude atteignable Δ donne un minorant $h_2^{-1}(\Delta)$ du TEB à Ève, comme indiqué

par l'inégalité suivante (conséquence de la concavité de la fonction h_2 et de l'inégalité de Jensen), pour tout $\breve{A}^n \in \mathcal{A}^n$ tel que $\breve{A}^n \multimap (J, E^n) \multimap A^n$ forment une chaîne de Markov :

$$\frac{1}{n} H(A^n | J E^n) \leq h_2 \left(\frac{1}{n} \sum_{i=1}^{n} \Pr \left\{ \breve{A}_i \neq A_i \right\} \right) .$$

Résultats numériques

À partir des inégalités de la proposition 2.16, nous calculons quelques triplets atteignables pour $\epsilon = 0.1$ et $\beta = h_2(\epsilon) \approx 0.469$ (voir le tableau 2.16). En cas de codage sans perte (colonnes 1 et 2 du tableau 2.2), la variable auxiliaire V est choisie égale à A ($\nu = 0$) ; la variable U permet bien d'atteindre une incertitude non-nulle à Ève. Supposons alors que le débit est limité à 80% de celui requis pour une reconstruction parfaite de la source (colonne 3). Cela induit une distorsion de 0.015 à Bob et une incertitude de 0.133 bit à Ève. Une légère augmentation du niveau de distorsion à Bob peut donc être exploitée par Alice pour atteindre des gains significatifs en termes d'incertitude à Ève (multiplication par un facteur 3 ici). Notons de plus que, pour des niveaux de distorsion supérieurs à 0.036, le schéma de Wyner-Ziv est optimal (voir la figure 2.16).

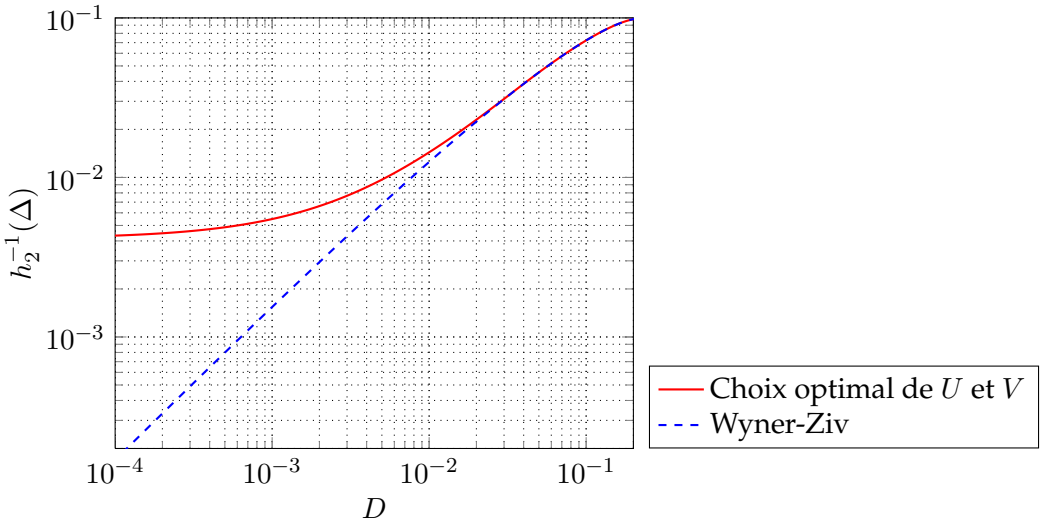


Figure 2.16 – $h_2^{-1}(\Delta)$ (minorant du TEB à Ève) en fonction du niveau de distorsion (et majorant du TEB) à Bob D ($\epsilon = 0.1$, $\beta = h_2(\epsilon) \approx 0.469$).

	Optimal	Slepian-Wolf	Optimal	Wyner-Ziv
Débit R	0.469	0.469	0.375	0.375
Distorsion D	0	0	0.015	0.015
Incertitude Δ	0.039	0	0.133	0.126
ν	0	0	0.031	0.031
μ	0.078	0	0.050	0

Tableau 2.2 – Quelques triplets atteignables et paramètres correspondants ($\epsilon = 0.1$, $\beta = h_2(\epsilon) \approx 0.469$).

2.7 Conclusion

Dans ce chapitre, nous avons défini et étudié le problème général du codage de source sous contrainte de sécurité, avec information adjacente codée au récepteur. Nous avons démontré des bornes intérieure et extérieure à la région atteignable correspondante. Ce problème peut être vu comme l'extension naturelle de celui de Berger et al. [11] en prenant en compte des contraintes de sécurité. Notons que ce dernier est un problème fondamental pour lequel le meilleur schéma de codage connu n'est pas optimal dans le cas général. De même, les bornes que nous avons proposées sont distinctes en général, mais la borne intérieure (atteignable) est optimale dans certains cas, en particulier pour le problème du codage de source avec information adjacente non codée, et celui de la compression sans perte distribuée. Il est intéressant de noter que, dans ces deux cas, fournir une description *commune* de la source aux deux récepteurs n'induit aucune perte ; l'information supplémentaire est destinée au récepteur légitime et considérée par l'espion comme des bits « bruts ». De plus, sous certaines conditions, le simple schéma de Wyner-Ziv (ou celui de Slepian-Wolf) peut atteindre la région toute entière, et le plus haut niveau de sécurité est garanti sans effort particulier.

Ces résultats ont été appliqués au codage avec perte de sources gaussiennes et binaires. Le modèle binaire considéré présente un intérêt particulier, car il n'y a pas toujours un récepteur moins bruité que l'autre. Un schéma de codage original est donc nécessaire. Dans le cas gaussien quadratique, les résultats de Oohama [119] suggèrent une région intérieure optimale dans certains cas. Une analyse plus approfondie avec des inégalités récentes [97, 136] pourrait permettre de démontrer la réciproque dans le cas général.

Dans ce chapitre, nous avons supposé qu'émetteurs et récepteurs sont connectés par des liens sans erreur à débit limité. Les canaux bruités peuvent cependant fournir une sécurité supplémentaire, comme dans le problème du canal *wiretap* [165]. Un résultat d'optimalité dans le cas de canaux et informations adjacentes dégradés a récemment été démontré [106]. Le problème plus général de la *transmission sécurisée d'une source via un canal bruité, avec information adjacente aux récepteurs* est étudié dans le chapitre 3 ci-après.

CHAPITRE 3

Transmission sécurisée d'une source via un canal bruité, avec information adjacente aux récepteurs

Résumé. Ce chapitre traite du problème de codage de source-canal pour les transmissions sécurisées, avec information adjacente aux récepteurs. Dans ce contexte, un émetteur (appelé Alice) souhaite compresser une source et l'envoyer via un canal bruité à un récepteur légitime (Bob), en satisfaisant simultanément des contraintes sur le niveau de distorsion à Bob, et sur l'incertitude d'un adversaire (Ève). Ce problème peut être vu comme la généralisation des problèmes de codage de source sous contrainte de sécurité, avec information adjacente non codée (étudié à la section 2.4), et du canal *wiretap*. Pour des canaux et informations adjacentes arbitraires, sont démontrées une borne extérieure générale pour la région débit-distorsion-incertitude, et une borne intérieure basée sur un schéma de codage purement numérique. Dans certains cas d'intérêt, ce schéma numérique est optimal, et le principe de séparation est satisfait. Cependant, un contre-exemple simple avec une source binaire montre qu'un schéma purement analogique peut faire mieux, et même être optimal. À partir de ces observations, en supposant une seule utilisation du canal par symbole de source (*matched-bandwidth*), un nouveau schéma hybride analogique/numérique est proposé. Dans le cas gaussien quadratique, lorsque seul l'espion dispose d'information adjacente, on démontre que cette stratégie est optimale ; de plus, elle fait mieux que les schémas numérique et analogique étudiés, et ne peut être égalée par une combinaison de ces derniers. Avec un codage approprié, toute différence statistique entre les informations adjacentes, les bruits des canaux, ainsi que la distorsion à Bob peuvent être pleinement exploitées en termes de sécurité.

3.1 Introduction

Considérons un système composé de trois nœuds (ou capteurs), chacun mesurant une source analogique. L'un deux (Alice) souhaite transmettre une version compressée de son observation à un second nœud (Bob) via un canal bruité (sans fil). Bob peut bien sûr utiliser sa propre observation comme information adjacente, pour décoder le message reçu et affiner son estimée de la source d'Alice. Le troisième nœud (Ève) est un espion : il peut écouter les messages envoyés par Alice via un autre canal bruité. Considérant que Ève n'est pas digne de confiance (c'est un ennemi, ou un capteur piraté en cours d'opération), Alice souhaite dévoiler aussi peu que possible sa source à cet adversaire.

Ce problème touche à des problématiques majeures de la théorie de l'information, parmi lesquelles la notion de sécurité (ou secret), et son application aux codages de source et de canal, le codage de source avec information adjacente, ainsi que le codage conjoint de source-canal pour la transmission de sources via des canaux bruités. La notion de sécurité, introduite dans la théorie de l'information par Shannon [140], a tout d'abord été utilisée pour les transmissions sécurisées via des canaux bruités par Wyner [165], qui a défini le canal *wiretap*, par la suite étendu par Csiszár et Körner [32]. D'autre part, le codage de source avec information adjacente a été introduit par Slepian et Wolf [143], et Wyner et Ziv [166]. Dans le chapitre 2, nous avons considéré des contextes similaires avec, en plus, un adversaire qui doit être maintenu aussi ignorant que possible à propos de la source transmise (voir la section 2.1 pour une revue de la littérature sur ce sujet).

La plupart des travaux existants considèrent séparément les codages de source et de canal pour les transmission sécurisées. Cependant, contrairement au cas des communications point-à-point [107, 139], il n'existe aucun résultat général de séparation pour de tels problèmes à plusieurs terminaux. Récemment, Merhav [106] a considéré le codage de source-canal pour les transmissions sécurisées, en supposant que l'information adjacente et le canal de Ève sont dégradés par rapport à ceux de Bob ; dans ce cas, il est montré que le principe de séparation est satisfait. Ce résultat pourrait indiquer que les schémas *numériques* sont bien adaptés aux problèmes des tranmissions sécurisées. D'autre part, il est bien connu que les codes *conjoints* sont essentiels pour les canaux de diffusion classiques [47, 155], et que les schémas hybrides analogiques/numériques sont utiles (par ex. pour gérer la connaissance imparfaite du rapport signal à bruit (*SNR mismatch*) dans les communications point-à-point [109, 161], mais aussi pour quelques problèmes à plusieurs terminaux [45,57,91]). En tirant avantage des stratégies analogiques *et* numériques, ces derniers pourraient aider à résoudre le problème de transmission sécurisée considéré dans un cas plus général, sans condition de « dégradation ».

Dans ce chapitre, nous étudions le codage de source-canal pour la transmission sécurisée d'une source via un canal bruité, en présence d'un adversaire, et avec information adjacente aux récepteurs (voir la figure 3.1). Ce problème peut être vu comme l'unification des problèmes de codage de source sous contrainte de sécurité, avec information adjacente aux décodeurs (étudié dans la section 2.4), et du canal *wiretap* [32,165]. L'objectif principal est de comprendre comment Alice peut dans le même temps tirer avantage des différences statistiques entre les informations adjacentes et entre les canaux pour révéler le moins d'information possible à Ève, et satisfaire la contrainte de distorsion de Bob. Notons que la difficulté centrale réside dans l'évaluation de l'incertitude à Ève. En effet, la présence d'information adjacente, qui peut être utilisée en même temps que la sortie du canal pour estimer la source, empêche l'application directe des résultats classiques de *secrecy capacity* [32]. Nous démontrons tout d'abord une borne extérieure à la région atteignable, appelée *région débit-distorsion-incertitude*, pour des canaux et informations adjacentes arbitraires. Nous proposons ensuite un schéma de codage purement numérique (qui combine le codage de source du chapitre 2 et le codage pour les canaux de diffusion avec messages confidentiels [32]) et donnons une expression simple (*single-letter*) de la

région correspondante. Ces deux bornes sont distinctes dans le cas général, mais nous démontrons à partir de celles-ci deux résultats d'optimalité lorsque (*i*) l'information adjacente de Bob est moins bruitée, et (*ii*) le canal de Ève est moins bruité. Dans les deux cas, le principe de séparation est satisfait, et les stratégies optimales correspondent respectivement à (*i*) un codage de *Wyner-Ziv* [166] suivi d'un codage pour le canal *wiretap* [32], et (*ii*) codage de source *securisé* (voir chapitre 2) suivi d'un codage de canal conventionnel [139]. Cependant, nous montrons à travers un contre-exemple simple, avec une source binaire, qu'un schéma purement analogique peut faire mieux que le schéma numérique, et même être optimal. Nous restreignons alors notre attention au cas où une seule utilisation du canal est autorisée par symbole de source (*matched-bandwidth*), et proposons un nouveau schéma hybride analogique/numérique pour simultanément tirer avantage des stratégies analogiques et numériques. Une expression simple (*single-letter*) de la région correspondante est démontrée. Dans le cas gaussien quadratique, lorsque seul l'adversaire dispose d'information adjacente, cette stratégie est optimale. Elle est plus performante que les schémas analogique et numérique (pris séparément, ou combinés par *time-sharing*). Nous considérons également la transmission d'une source binaire avec des informations adjacentes CBE/CBS (comme dans la section 2.6.2) via un canal *wiretap* de type II. Le schéma hybride analogique/numérique se révèle également utile dans ce contexte.

La suite de ce chapitre est organisée de la manière suivante. Les principales définitions, ainsi que la borne extérieure générale, sont données dans la section 3.2. La section 3.3 est consacrée à la région intérieure basée sur un schéma purement numérique, dont la démonstration est donnée à la section 3.4. La transmission d'une source binaire via un canal *wiretap* de type II est étudiée à la section 3.5, fournissant un contre-exemple à l'optimalité du schéma numérique. Une région atteignable basée sur un schéma hybride analogique/numérique est proposée à la section 3.6, et démontrée à la section 3.7. La section 3.8 (resp. 3.9) présente une application à la transmission d'une source binaire via un canal *wiretap* de type II (resp. d'une source gaussienne via un canal *wiretap* gaussien).

Notations

Pour toute suite $(x_i)_{i\in\mathbb{N}^*}$, x_k^n désigne la collection $(x_k, x_{k+1}, \dots, x_n)$. L'entropie est notée $H(\cdot)$, et l'information mutuelle $I(\cdot;\cdot)$. On désigne les ensembles typiques et conditionnellement typiques par $T_\delta^n(X)$ et $T_\delta^n(Y|x^n)$, resp. (voir l'annexe A). Soient X, Y et Z trois variables aléatoires de distribution p. Si $p(x|yz) = p(x|y)$ pour tous x, y, z, alors elles forment une chaîne de Markov, notée $X \multimap Y \multimap Z$. La variable aléatoire Y est dite moins bruitée que Z par rapport à X si $I(U;Y) \geq I(U;Z)$ pour toute variable aléatoire U telle que $U \multimap X \multimap (Y,Z)$ forment une chaîne de Markov. Cette relation est notée $Y \succeq_X Z$. L'ensemble des nombres réels positifs est noté $\mathbb{R}_+$. Pour tout $x \in \mathbb{R}$, $[x]_+$ désigne $\max\{0\,;x\}$. Les logarithmes sont pris en base 2 et notés $\log(\cdot)$. L'entropie binaire est définie sur $[0\,;1]$ par $h_2(x) = -x\log(x) - (1-x)\log(1-x)$. Son inverse h_2^{-1} est définie sur $[0\,;1]$ et à valeurs dans $[0\,;\frac{1}{2}]$. Pour tous $a, b \in [0\,;1]$, $a \star b = a(1-b) + (1-a)b$. La distribution de Bernoulli de paramètre u est notée $\mathcal{B}(u)$.

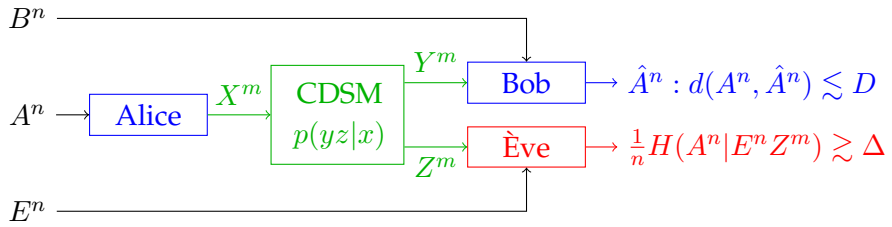


Figure 3.1 – Transmission sécurisée avec information adjacente aux récepteurs.

3.2 Définitions et borne extérieure générale

3.2.1 Définitions

Dans cette section, nous formalisons le contexte représenté à la figure 3.1. Soient $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{X}$, $\mathcal{Y}$, et $\mathcal{Z}$ six ensembles finis. Alice, Bob et Ève observent les suites de variables aléatoires $(A_i)_{i\in\mathbb{N}^*}$, $(B_i)_{i\in\mathbb{N}^*}$ et $(E_i)_{i\in\mathbb{N}^*}$, respectivement, à valeurs dans $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{E}$, resp. Pour tout $i \in \mathbb{N}^*$, les variables aléatoires A_i, B_i et E_i sont distribuées selon $p(abe)$ sur $\mathcal{A}\times\mathcal{B}\times\mathcal{E}$. De plus, elles sont indépendantes au cours du temps i. Alice peut communiquer avec Bob et Ève via un canal discret sans mémoire (CDSM) d'entrée X sur $\mathcal{X}$, et de sorties Y, Z sur $\mathcal{Y}$, $\mathcal{Z}$, respectivement. Ce canal est défini par la probabilité de transition $p(yz|x)$.

Soit $d\colon \mathcal{A}\times\mathcal{A} \to [0\,; d_{\max}]$ une mesure de distorsion finie, c.-à-d. telle que $0 \le d_{\max} < \infty$. On note également d la distorsion moyenne des composantes sur $\mathcal{A}^n \times \mathcal{A}^n$: pour tous $a^n, b^n \in \mathcal{A}^n$, $d(a^n, b^n) \triangleq \frac{1}{n}\sum_{i=1}^n d(a_i, b_i)$.

Définition 3.1 (Code)**.** Un code (n, m) pour le codage de source-canal est défini dans ce contexte par

- une fonction (stochastique) d'encodage à Alice $F\colon \mathcal{A}^n \to \mathcal{X}^m$, définie par une probabilité de transition $P_F(x^m|a^n)$,
- une fonction de décodage à Bob $g\colon \mathcal{B}^n \times \mathcal{Y}^m \to \mathcal{A}^n$.

Le débit d'un tel code est défini comme le nombre d'utilisation du canal par symbole de source $\frac{m}{n}$.

Définition 3.2 (Atteignabilité)**.** Un triplet $(k, D, \Delta) \in \mathbb{R}_+^3$ est dit *atteignable* si, pour tout $\varepsilon > 0$, il existe un code (n, m), (F, g), tel que :

$$\begin{aligned} \frac{m}{n} &\le k + \varepsilon\,, \\ \mathbb{E}\big[d(A^n, g(B^n, Y^m))\big] &\le D + \varepsilon\,, \\ \frac{1}{n} H(A^n|E^n Z^m) &\ge \Delta - \varepsilon\,, \end{aligned}$$

avec la sortie de l'encodeur placée en entrée du canal ($X^m = F(A^n)$).
L'ensemble des triplets atteignables est noté $\mathcal{R}^*$ et appelé *région débit-distorsion-incertitude*.

Remarque 3.1. La région $\mathcal{R}^*$ est fermée et convexe.

Remarque 3.2. Les quantités apparaissant dans la définition 3.2 dépendent uniquement des distributions marginales $p(ae)$, $p(ab)$, $p(y|x)$ et $p(z|x)$. Il en est de même pour les résultats ci-dessous, qui fournissent des bornes intérieure et extérieure à la région $\mathcal{R}^*$.

3.2.2 Borne extérieure générale

Le théorème suivant donne une borne extérieure à la région $\mathcal{R}^*$: il définit $\mathcal{R}_{\text{ext}} \supseteq \mathcal{R}^*$.

Théorème 3.1 (Borne extérieure)**.** *Si (k, D, Δ) est atteignable, alors il existe des variables aléatoires U, V, Q, T, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$ (resp.) de loi jointe $p(uvqtabexyz) = p(uv|a)p(abe)\,p(q|t)p(t)p(x|t)p(yz|x)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$I(V;A|B) \leq kI(T;Y)\,, \tag{3.1}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\,, \tag{3.2}$$

$$\Delta \leq H(A|UE) - \Big[I(V;A|B) - I(U;A|B) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+\,. \tag{3.3}$$

Démonstration. Voir l'annexe E.1. □

3.3 Schéma numérique

Dans cette section, nous proposons un schéma de codage numérique pour les transmissions sécurisées, et donnons la région intérieure *single-letter* correspondante (théorème 3.2). Ce schéma est optimal sous certaines conditions (propositions 3.3 et 3.4).

3.3.1 Énoncé général

Le théorème suivant donne une région intérieure à $\mathcal{R}^*$: il définit la région $\mathcal{R}_{\text{num}} \subseteq \mathcal{R}^*$. Son atteignabilité vient de la combinaison du codage de source sous contrainte de sécurité du chapitre 2 et du codage pour les canaux de diffusion avec messages confidentiels [32]. Ce schéma sera appelé le *schéma numérique*.

Théorème 3.2 (Schéma numérique)**.** *Un triplet $(k, D, \Delta) \in \mathbb{R}_+^3$ est atteignable s'il existe des variables aléatoires U, V, Q, T, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$ (resp.) de loi jointe $p(uvqtabexyz) = p(u|v)p(v|a)p(abe)\,p(q|t)p(t)p(x|t)p(yz|x)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$I(U;A|B) \leq kI(Q;Y)\,, \tag{3.4}$$

$$I(V;A|B) \leq kI(T;Y)\,, \tag{3.5}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\,, \tag{3.6}$$

$$\Delta \leq H(A|UE) - \Big[I(V;A|UB) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+\,. \tag{3.7}$$

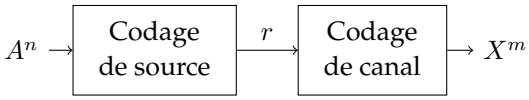


Figure 3.2 – Séparation traditionnelle.

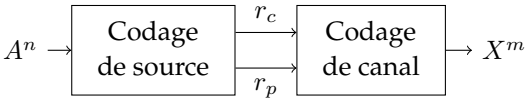


Figure 3.3 – Système proposé (Séparation « opérationnelle »).

Démonstration. Voir la section 3.4. □

Les inégalités (3.4) et (3.5) correspondent à des conditions suffisantes pour la transmission de deux descriptions U, V via les variables de canal Q, T, respectivement. La première couche (U, Q) peut être vue comme un message *commun*, connu à Ève, comme l'indique le terme $H(A|UE)$ dans (3.7). La seconde couche (V, T) forme un message *privé*, (partiellement) protégé par l'ajout d'un bruit aléatoire indépendant [32, 90]. Le terme entre crochets de l'équation (3.7) correspond à l'information que Ève peut toujours obtenir sur cette couche protégée.

Notons que les bornes intérieure $\mathcal{R}_{\text{num}}$ et extérieure $\mathcal{R}_{\text{ext}}$ sont disjointes en général :

- La condition (3.4) du théorème 3.2, nécessaire dans notre schéma pour caractériser l'incertitude à Ève, peut ne pas être optimale dans le cas général (voir le théorème 3.1).
- La chaîne de Markov $U \multimap V \multimap A \multimap (B, E)$ est une hypothèse du théorème 3.2 alors que seule $(U, V) \multimap A \multimap (B, E)$ est démontrée pour des codes arbitraires dans le théorème 3.1.

Nous donnons dans la section 3.3.3 plusieurs cas où la région $\mathcal{R}_{\text{num}}$ est optimale.

3.3.2 Schéma basé sur une séparation « opérationnelle »

Dans les schémas *séparés* traditionnels, deux composants *indépendants* réalisent successivement le codage de source et le codage de canal (voir la figure 3.2). La stratégie qui permet d'atteindre la région $\mathcal{R}_{\text{num}}$ ne satisfait pas ce principe de séparation : l'étape de codage de source produit deux indices distincts (deux couches), traités ensuite par un code pour les canaux de diffusion avec messages confidentiels [32] (voir la section 3.4). Il en résulte deux composants *autonomes* (mais non indépendants), correspondant à des variables de source et de canal statistiquement indépendantes (comme dans [155] pour le codage de Slepian-Wolf via les canaux de diffusion). Autrement dit, il y a séparation « opérationnelle » (voir la figure 3.3). Par exemple, l'inégalité (3.4) dans le théorème 3.2 empêche de choisir séparément les variables U et Q qui maximisent l'incertitude à Ève (3.7) ; il faut les optimiser en même temps.

3.3.3 Cas particuliers

Dans cette section, nous caractérisons l'optimalité de la borne intérieure $\mathcal{R}_{\text{num}}$ dans certains cas d'intérêt.

3.3.3.1 Information adjacente de Bob moins bruitée ($B \succeq_A E$)

Si l'information adjacente de Bob est *moins bruitée* que celle de Ève, alors la stratégie optimale se résume à utiliser le schéma de *Wyner-Ziv* [166] suivi d'un codage pour le canal *wiretap* [32], et le principe de séparation est satisfait (voir figure 3.2) :

Proposition 3.3. *Si $B \succeq_A E$, $(k, D, \Delta) \in \mathbb{R}_+^3$ est atteignable si et seulement si il existe des variables aléatoires V, Q, T, X sur les ensembles finis $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$ (resp.) de loi jointe $p(vqtabexyz) = p(v|a)p(abe)\,p(q|t)p(t)p(x|t)p(yz|x)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$\begin{aligned} &I(V;A|B) \leq kI(T;Y)\ , \\ &D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\ , \\ &\Delta \leq H(A|E) - \Big[I(V;A|B) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+ . \end{aligned}$$

Démonstration. Voir la section 3.3.3 dans la partie II. □

Si les observations de Ève (information adjacente et sortie de canal) sont des versions dégradées de celles de Bob, c'est-à-dire si $A \multimap B \multimap E$ et $X \multimap Y \multimap Z$ forment des chaînes de Markov, alors la proposition 3.3 est une conséquence des résultats de [106]. Dans ce cas, la variable Q est choisie constante, et $T = X$.

3.3.3.2 Canal de Ève moins bruité ($Z \succeq_X Y$)

Si le canal de Ève est moins bruité que celui de Bob, alors la stratégie optimale se résume à utiliser un codage de source *sécurisé* (voir le chapitre 2) suivi d'un codage de canal traditionnel pour les communications point-à-point [139], et le principe de séparation est satisfait (voir figure 3.2) :

Proposition 3.4. *Si $Z \succeq_X Y$, $(k, D, \Delta) \in \mathbb{R}_+^3$ est atteignable si et seulement si il existe des variables aléatoires U, V, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$ (resp.) de loi jointe $p(uvabexyz) = p(u|v)p(v|a)p(abe)\,p(x)p(yz|x)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$\begin{aligned} &I(V;A|B) \leq kI(X;Y)\ , \\ &D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\ , \\ &\Delta \leq H(A|VB) + I(A;B|U) - I(A;E|U)\ . \end{aligned}$$

Démonstration. Voir la section 3.3.3 dans la partie II. □

3.4 Démonstration du théorème 3.2 (Schéma numérique)

Soient quatre variables aléatoires U, V, Q, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{X}$, respectivement, telles que $p(uvqabexyz) = p(u|v)p(v|a)p(abe)\,p(q|x)p(x)p(yz|x)$, une fonction $\hat{A}\colon \mathcal{V}\times\mathcal{B}\to\mathcal{A}$, et un triplet $(k, D, \Delta)\in\mathbb{R}_+^3$. Nous décrivons dans cette section un schéma qui atteint (sous certains conditions) le triplet (k, D, Δ) : pour tout $\varepsilon > 0$, nous construisons un code (n, m), (F, g), tel que

$$\begin{aligned}\frac{m}{n} &\leq k+\varepsilon\,,\\ \mathbb{E}\big[d\big(A^n, g(B^n, Y^m)\big)\big] &\leq D+\varepsilon\,,\\ \frac{1}{n}\,H(A^n|E^n Z^m) &\geq \Delta-\varepsilon\,.\end{aligned}$$

Soient $\varepsilon > 0$, $R_1, R_2, R_c, R_p, R_f \in \mathbb{R}_+^*$, $S_1 \geq R_1$, $S_2 \geq R_2$ tels que

$$R_f < (k+\varepsilon)\,I(X;Z|Q)\,. \tag{3.8}$$

On suppose qu'Alice dispose d'une source aléatoire locale r_f (indépendante et uniformément distribuée) de débit R_f, et on pose $m = \lfloor n(k+\varepsilon)\rfloor$. Dans les paragraphes suivants, nous exposons les principes de la stratégie de codage utilisée. Les détails sont donnés dans la section 3.4 de la partie II.

3.4.1 Encodage

De même que dans le chapitre 2, Alice compresse la source A en U, puis en V, via deux dictionnaires de séquences typiques u^n et v^n. Pour tirer parti de l'information adjacente à Bob, elle sépare aléatoirement (à chaque étape) ces mots de code en plusieurs groupes (*random binning*), comme dans le codage de Wyner-Ziv [166] (voir la figure 2.7). D'après les propriétés des séquences typiques, on peut montrer que la probabilité que cette étape échoue tend vers zéro quand n tend vers l'infini, si $S_1 > I(U;A)$ et $S_2 > I(V;A|U)$.

Les indices correspondants $(r_1, r_2) \in \{1,\dots,2^{nR_1}\}\times\{1,\dots,2^{nR_2}\}$ sont alors transformés en $(r_c, r_p) \in \{1,\dots,2^{nR_c}\}\times\{1,\dots,2^{nR_p}\}$ via une bijection M telle que $r_1 = M'(r_c)$

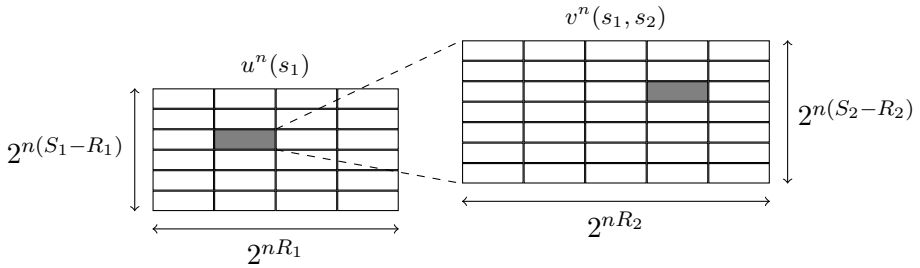


Figure 3.4 – Schéma numérique – Dictionnaire « source ».

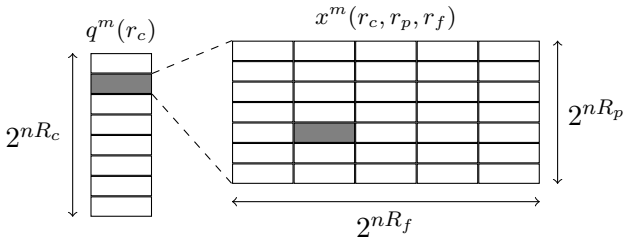


Figure 3.5 – Schéma numérique – Dictionnaire « canal ».

pour une certaine fonction M'. Cette opération est possible si :

$$R_1 + R_2 = R_c + R_p \,, \tag{3.9}$$

$$R_1 \leq R_c \,. \tag{3.10}$$

Pour transmettre les deux nouveaux indices, Alice utilise un code pour les canaux de diffusion avec messages confidentiels [32], où r_c est le message commun et r_p le message privé protégé par le bruit indépendant r_f. Pour ce faire, Alice utilise deux dictionnaires de séquences typiques q^m et x^m (voir la figure 3.5).

Au final, Alice envoie $X^m = F(A^n) \triangleq x^m(r_c, r_p, r_f)$ sur le canal.

3.4.2 Décodage

À partir de l'information adjacente B^n et de la sortie du canal Y^m, Bob décode les variables U et V de la manière suivante.

Tout d'abord, il décode r_C en cherchant l'unique mot de code q^m typique avec Y^m. Puis, de la même manière, il décode (r_p, r_f) en cherchant l'unique x^m typique avec Y^m (sachant q^m). D'après un raisonnement standard en codage de canal, ces deux étapes échouent avec une faible probabilité si $R_c < (k+\varepsilon)I(Q;Y)$ et $R_p + R_f < (k+\varepsilon)I(X;Y|Q)$.

Bob calcule alors $(r_1, r_2) = M^{-1}(r_c, r_p)$, et cherche l'unique mot de code u^n typique avec B^n dont le numéro de groupe est r_1, puis l'unique v^n typique avec B^n (sachant u^n) dont le numéro de groupe est r_2. Cette opération réussit avec une grande probabilité si $S_1 - R_1 < I(U;B)$ et $S_2 - R_2 < I(V;B|U)$.

Bob peut calculer l'estimée $g(B^n, Y^m) \in \mathcal{A}^n$ à partir de la relation suivante, pour tout $i = \{1, \ldots, n\}$:

$$g_i(B^n, Y^m) \triangleq \hat{A}(v_i, B_i) \,.$$

La distorsion moyenne de cette estimée peut être facilement caractérisée. Pour n assez grand, elle vérifie l'inégalité suivante :

$$\mathbb{E}\Big[d\big(A^n, g(B^n, Y^m)\big)\Big] \leq \mathbb{E}\big[d(A, \hat{A}(V, B))\big] + \varepsilon \,.$$

La condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big]$ est donc suffisante pour atteindre un niveau de distorsion $D + \varepsilon$ à Bob.

3.4.3 Incertitude à Ève

L'incertitude à Ève (moyennée sur l'ensemble des dictionnaires possibles) peut s'écrire de la manière suivante :

$$H(A^n|E^nZ^m) = \underbrace{H(A^n|r_cr_pE^nZ^m)}_{E_s} + \underbrace{I(A^n;r_cr_p|E^nZ^m)}_{E_c} . \tag{3.11}$$

Le terme de « source » E_s peut être étudié de la même manière que l'incertitude de la section 2.3.3 :

$$\begin{aligned} E_s &= H(A^n|r_1r_2E^n) \\ &= H(A^n|r_1E^n) - H(r_2) + I(r_2;r_1E^n) \\ &\geq nH(A|UE) - n\,\tfrac{\varepsilon}{4} - nR_2 + I(r_2;E^n|r_1) . \end{aligned} \tag{3.12}$$

Le terme de « canal » E_c s'écrit

$$\begin{aligned} E_c &= H(r_cr_p|E^nZ^m) \\ &= H(r_p|r_cZ^m) + H(r_c|Z^m) - I(r_cr_p;E^n|Z^m) . \end{aligned} \tag{3.13}$$

Le premier terme du membre de droite de (3.13) correspond à l'incertitude (du message *privé*, sachant le message *commun* et la sortie du canal) dans le problème du canal *wiretap*. En suivant [32, Section IV], [90, Section 2.3], et grâce à la contrainte (3.8), on peut montrer l'inégalité suivante (pour m suffisamment grand) :

$$H(r_p|r_cZ^m) \geq n(R_p + R_f) - mI(X;Z|Q) - 1 - n\,\tfrac{\varepsilon}{2} . \tag{3.14}$$

les équations (3.11)–(3.14) donnent ensemble

$$\begin{aligned} H(A^n|E^nZ^m) \geq\ & nH(A|UE) - nR_2 + n(R_p + R_f) - mI(X;Z|Q) \\ & + I(r_2;E^n|r_1) + H(r_c|Z^m) - I(r_cr_p;E^n|Z^m) - n\,\tfrac{3\varepsilon}{4} - 1 . \end{aligned} \tag{3.15}$$

En utilisant les caractéristiques de la procédure proposée (par ex., $r_1 = M'(r_c)$ pour une certaine fonction M'), on peut montrer que

$$I(r_2;E^n|r_1) + H(r_c|Z^m) - I(r_cr_p;E^n|Z^m) \geq 0 .$$

L'inégalité (3.15) donne donc (pour m suffisamment grand) :

$$\frac{1}{n}H(A^n|E^nZ^m) \geq H(A|UE) - R_2 + R_p + R_f - \frac{m}{n}\,I(X;Z|Q) - \varepsilon ,$$

et la condition $\Delta \leq H(A|UE) - R_2 + R_p + R_f - (k+\varepsilon)I(X;Z|Q)$ est suffisante pour atteindre l'incertitude $\Delta - \varepsilon$.

3.4.4 Résumé des conditions suffisantes

Les équations suivantes fournissent des conditions suffisantes pour l'atteignabilité du triplet $(k, D, \Delta) \in \mathbb{R}_+^3$: pour tout $\varepsilon > 0$,

$$\begin{cases} R_1, R_2, R_c, R_p, R_f > 0 \\ R_1 + R_2 = R_c + R_p \\ \qquad R_1 \leq R_c \\ \qquad S_1 \geq R_1 \\ \qquad S_2 \geq R_2 \\ \qquad S_1 > I(U;A) \\ \qquad S_2 > I(V;A|U) \\ \qquad R_c < (k+\varepsilon) I(Q;Y) \\ R_p + R_f < (k+\varepsilon) I(X;Y|Q) \\ S_1 - R_1 < I(U;B) \\ S_2 - R_2 < I(V;B|U) \\ \qquad R_f < (k+\varepsilon) I(X;Z|Q) \\ \qquad D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] \\ \qquad \Delta \leq H(A|UE) - R_2 + R_p + R_f - (k+\varepsilon) I(X;Z|Q) \end{cases}$$

L'algorithme d'élimination de Fourier-Motzkin [156] conduit alors au système suivant :

$$\begin{cases} I(U;A|B) < (k+\varepsilon) I(Q;Y) \\ I(V;A|B) < (k+\varepsilon) I(X;Y) \\ \qquad D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] \\ \qquad \Delta < H(A|UE) \\ \qquad \Delta < H(A|UE) - I(V;A|UB) + (k+\varepsilon)\Big(I(X;Y|Q) - I(X;Z|Q)\Big) \end{cases}$$

3.4.5 Ajout d'un pré-canal

Pour toute variable aléatoire T sur un ensemble fini $\mathcal{T}$ telle que $T \multimap X \multimap (Y, Z)$ forment une chaîne de Markov, on peut utiliser le schéma décrit ci-dessus pour le CDSM $T \mapsto$

(Y, Z) à la place de $X \mapsto (Y, Z)$. Dans ce cas, les conditions suffisantes ci-dessus s'écrivent

$$\begin{cases} I(U;A|B) < (k+\varepsilon) I(Q;Y) \\ I(V;A|B) < (k+\varepsilon) I(T;Y) \\ \qquad D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] \\ \qquad \Delta < H(A|UE) \\ \qquad \Delta < H(A|UE) - I(V;A|UB) + (k+\varepsilon)\Big(I(T;Y|Q) - I(T;Z|Q)\Big) \end{cases}$$

Comme la région $\mathcal{R}^*$ est fermée, cela démontre le théorème 3.2. □

3.5 Transmission d'une source binaire avec informations adjacentes CBE/CBS via un canal *wiretap* de type II

3.5.1 Modèle

Considérons le modèle introduit à la section 2.6.2 et représenté à la figure 3.6, où la source est binaire, uniformément distribuée ($A \sim \mathcal{B}\left(\frac{1}{2}\right)$), et l'information adjacente de Bob (resp. Ève) est produite à partir de A via un canal binaire à effacement (CBE) de probabilité d'effacement $\beta \in \,]0\,;1]$ (resp. un canal binaire symétrique (CBS) de probabilité d'erreur $\epsilon \in [0\,;\frac{1}{2}]$). Rappelons que, en fonction des valeurs des paramètres (β, ϵ), les informations adjacentes vérifient les propriétés résumées par la figure 3.8 [112].

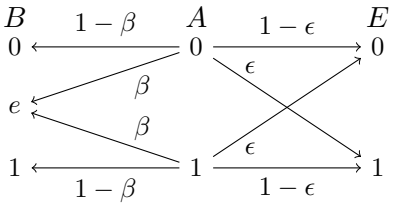


Figure 3.6 – Source binaire avec informations adjacentes CBE/CBS.

Le canal de communication est un canal *wiretap* (binaire) de type II [165] : il est sans bruit entre Alice et Bob, et binaire symétrique entre Alice et Ève, avec une probabilité d'erreur $\zeta \in [0\,;\frac{1}{2}]$ (voir la figure 3.7).

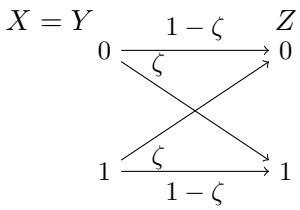


Figure 3.7 – Canal *wiretap* de type II.

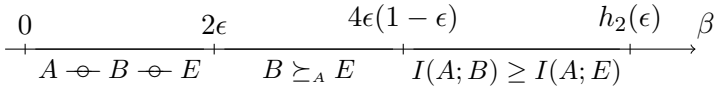


Figure 3.8 – Propriétes des informations adjacentes en fonction de (β, ϵ).

Dans cette section, nous nous concentrons sur le cas de la reconstruction *sans perte* à Bob (d est la distance de Hamming et $D = 0$) et autorisons une seule utilisation de canal par symbole de source (*matched bandwidth* : $k = 1$).

3.5.2 Performances de quelques schémas de codage

La proposition suivante est une conséquence du théorème 3.1.

Proposition 3.5 (Borne extérieure). *Si $(k = 1, D = 0, \Delta)$ est atteignable, alors il existe $u, q \in [0\,;\frac{1}{2}]$ tels que*

$$\Delta \leq h_2(\epsilon) + h_2(u) - h_2(\epsilon \star u) - \Big[\beta h_2(u) - \Big(h_2(\zeta) + h_2(q) - h_2(\zeta \star q)\Big)\Big]_+ .$$

Démonstration. Cette proposition se démontre de la même manière que la réciproque de la proposition 3.6 ci-dessous, donnée en annexe E.2. Les détails sont omis. □

La proposition suivante donne une expression simple de la région $\mathcal{R}_{\text{num}}$.

Proposition 3.6 (Schéma numérique). $(k = 1, D = 0, \Delta) \in \mathcal{R}_{num}$ *si et seulement si il existe $u, q \in [0\,;\frac{1}{2}]$ tels que*

$$\begin{aligned} &\beta(1 - h_2(u)) \leq 1 - h_2(q) \ , \\ &\Delta \leq h_2(\epsilon) + h_2(u) - h_2(\epsilon \star u) - \Big[\beta h_2(u) - \Big(h_2(\zeta) + h_2(q) - h_2(\zeta \star q)\Big)\Big]_+ . \end{aligned}$$

Démonstration. La réciproque est démontrée en annexe E.2.

L'atteignabilité est une conséquence du théorème 3.2 en choisissant les variables auxiliaires de la manière suivante (les détails sont omis) : $V = A$; $X \sim \mathcal{B}\left(\frac{1}{2}\right)$; U (resp. Q) est produit à partir de A (resp. X) via un CBS de probabilité d'erreur $u \in [0\,;\frac{1}{2}]$ (resp. $q \in [0\,;\frac{1}{2}]$). □

Notons que si $\beta \leq 4\epsilon(1-\epsilon)$, alors $B \succeq_A E$, et la proposition 3.3 s'applique ; autrement dit, la borne intérieure ci-dessus est optimale, et le principe de séparation est satisfait.

Dans la suite de cette section, nous comparons le schéma numérique à une méthode purement analogique consistant à placer directement la source en entrée du canal. La proposition suivante en donne les performances.

Proposition 3.7 (Schéma analogique). $(k = 1, D = 0, \Delta) \in \mathbb{R}_+^3$ *est atteignable avec un schéma analogique si*

$$\Delta \leq h_2(\epsilon) + h_2(\zeta) - h_2(\zeta \star \epsilon) .$$

Démonstration. Prendre $X = A$ donne une distorsion nulle à Bob (puisque $Y = X$) et une incertitude $H(A|EZ)$ à Ève. Par des manipulations standard, on obtient aisément les expressions ci-dessus. Les détails sont omis. □

3.5.3 Contre-exemple à l'optimalité du théorème 3.2

Supposons à présent que Bob n'a pas d'information adjacente ($\beta = 1$), et prenons $\epsilon = \zeta = 0.1$, de sorte que $A \multimap E \multimap B$ et $X \multimap Y \multimap Z$ forment des chaînes de Markov, et ni la proposition 3.3, ni la proposition 3.4 ne s'applique.

Ce contexte fournit un contre-exemple à l'optimalité de la région intérieure du théorème 3.2 : une optimisation numérique des paramètres u et q dans la proposition 3.6 indique que le schéma numérique atteint une incertitude $\Delta = 0.056$, alors que le schéma analogique de la proposition 3.7 atteint $\Delta = 0.258$. De plus, cette valeur coïncide avec la région extérieure de la proposition 3.5 : dans ce cas, le schéma analogique « naïf » (sans prise en compte de la sécurité) est optimal. Ceci montre qu'une approche *conjointe* source-canal peut atteindre de meilleures performances dans certains cas.

3.6 Codage hybride

La section précédente montre l'utilité des schémas *analogiques*. En accord avec ces observations, nous proposons ici un schéma *hybride analogique/numérique* qui donne une nouvelle région intérieure $\mathcal{R}_{\text{hyb}}$ (théorème 3.8) dans le cas *matched-bandwidth* ($k = 1$).

3.6.1 Énoncé général

Les canaux $A \mapsto B$ et $X \mapsto Y$ peuvent ensemble être vus comme un canal à état d'entrée X, état A et sortie (B, Y). Alice et Bob forment alors un système de communication où l'état du canal est connu (de manière non causale) à l'émetteur (ECCE). Voir la figure 3.9. Le schéma proposé consiste à envoyer un bruit numérique indépendant r_f en utilisant un codage de Gelfand-Pinsker [48] pour ce canal à état équivalent.

Théorème 3.8 (Schéma hybride)**.** *Un triplet $(k = 1, D, \Delta) \in \mathbb{R}_+^3$ est atteignable s'il existe des variables aléatoires U, V, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$ (resp.) de loi jointe $p(uvabexyz) = p(u|v)p(vx|a)\,p(abe)p(yz|x)$, $x = x(v, a)$, et une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \times \mathcal{Y} \to \mathcal{A}$, vérifiant les inégalités suivantes :*

$$I(U; A) \leq I(U; BY)\,, \tag{3.16}$$

$$I(V; A|U) \leq I(V; BY|U)\,, \tag{3.17}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big]\,, \tag{3.18}$$

$$\Delta \leq H(A|UE) - I(V; A|U) - I(X; Z|UE) + \min\Big\{I(V; BY|U)\,; I(V; AZ|U)\Big\}\,. \tag{3.19}$$

Démonstration. Voir la section 3.7. □

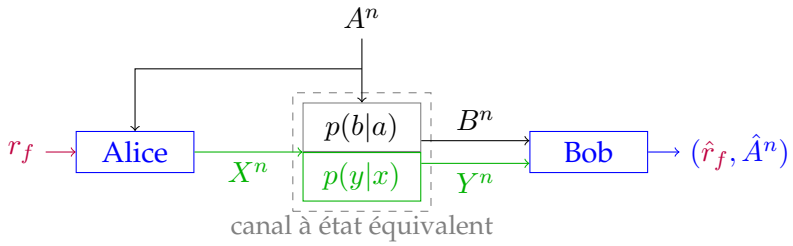


Figure 3.9 – Alice et Bob formant un système avec canal à état et ECCE.

Les inégalités (3.16), (3.17) correspondent à des conditions suffisantes pour la transmission des descriptions U, V de A à Bob. La première couche U peut être vue comme un message *commun*, considéré connu par Ève, comme le montre le terme $H(A|UE)$ de (3.19). Le bruit aléatoire numérique r_f aide ici à protéger la seconde couche V.

3.6.2 Cas particuliers

3.6.2.1 Schémas analogiques

Le schéma hybride proposé peut se simplifier en un code purement analogique (comme celui de la proposition 3.7). La région $\mathcal{R}_{\text{hyb}}$ contient donc des triplets qui ne sont pas dans $\mathcal{R}_{\text{num}}$: $\mathcal{R}_{\text{hyb}} \not\subset \mathcal{R}_{\text{num}}$.

3.6.2.2 Schémas numériques

En définissant les variables du théorème 3.8 comme des paires de composantes de source et de canal indépendantes, on peut obtenir la structure des variables du théorème 3.2. Cependant, ces variables n'en vérifient pas toutes les inégalités, et donc $\mathcal{R}_{\text{num}} \not\subset \mathcal{R}_{\text{hyb}}$.

3.7 Démonstration du théorème 3.8 (Schéma hybride)

Soient trois variables aléatoire U, V, X sur les ensembles finis $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, respectivement, telles que $p(uvabexyz) = p(u|v)p(vx|a)p(abe)p(yz|x)$, $x = x(v,a)$, une fonction $\hat{A}\colon \mathcal{V} \times \mathcal{B} \times \mathcal{Y} \to \mathcal{A}$, et une paire $(D, \Delta) \in \mathbb{R}_+^2$. Nous décrivons dans cette section un schéma qui atteint (sous certaines conditions) le triplet $(k = 1, D, \Delta)$: pour tout $\varepsilon > 0$, nous construisons un code (n, n), (F, g), tel que

$$\mathbb{E}\big[d\big(A^n, g(B^n, Y^n)\big)\big] \leq D + \varepsilon\,,$$
$$\frac{1}{n} H(A^n|E^n Z^n) \geq \Delta - \varepsilon\,.$$

Soient $\varepsilon > 0$, $R_1, R_2, R_f \in \mathbb{R}_+^*$ tels que

$$R_2 + R_f < I(V; AZ|U)\,. \tag{3.20}$$

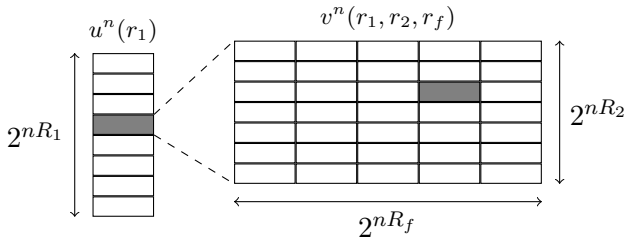


Figure 3.10 – Schéma hybride – Dictionnaire.

On suppose qu'Alice dispose d'une source aléatoire locale r_f (indépendante et uniformément distribuée) de débit R_f. Dans les paragraphes suivants, nous exposons les principes de la stratégie de codage utilisée. Les détails sont donnés dans la section 3.7 de la partie II.

3.7.1 Encodage

Alice compresse tout d'abord la source A en U, puis en V, via deux dictionnaires de séquences typiques u^n et v^n. Le bruit numérique r_f est également transmis en V, à la Gelfand-Pinsker [48], pour tirer parti du canal potentiellement meilleur de Bob et empêcher Ève de décoder la totalité du message (voir la figure 3.10). D'après les propriétés des séquences typiques, on peut montrer que la probabilité que cette étape échoue tend vers zéro quand n tend vers l'infini, si $R_1 > I(U;A)$ et $R_2 > I(V;A|U)$.

Finalement, Alice envoie $X^n = F(A^n)$ défini par la relation suivante, pour tout $i = \{1, \ldots, n\}$:

$$X_i \triangleq x(v_i(r_1, r_2, r_f), A_i) \; .$$

3.7.2 Décodage

À partir de l'information adjacente B^n et de la sortie du canal Y^n, Bob décode les variables U et V de la manière suivante.

Tout d'abord, il cherche l'unique mot de code u^n typique avec (B^n, Y^n), puis l'unique mot de code v^n typique avec (B^n, Y^n) (sachant u^n). Notons que la technique traditionnelle de *random coding*, qui permet d'analyser la probabilité d'erreur des procédures de décodage, ne peut être appliquée ici (voir [84, 91]). En effet, dans ce schéma hybride, un seul dictionnaire joue les deux rôles de dictionnaire de source et de dictionnaire de canal. Pour une certaine séquence a^n, les indices (r_1, r_2) dépendent donc de tous les mots de code, et la moyenne sur l'ensemble des dictionnaires possibles ne peut être calculée de la manière habituelle. On peut cependant démontrer, en suivant un raisonnement similaire à celui de [91], que la procédure de décodage décrite ci-dessus échoue avec une faible probabilité si $R_1 < I(U;BY)$ et $R_2 + R_f < I(V;BY|U)$.

Bob peut alors calculer l'estimée $g(B^n, Y^n) \in \mathcal{A}^n$ à partir de la relation suivante, pour tout $i = \{1, \ldots, n\}$:

$$g_i(B^n, Y^n) \triangleq \hat{A}(v_i(r_1, r_2, r_f), B_i, Y_i) \; .$$

La distorsion moyenne de cette estimée peut être facilement caractérisée. Pour n assez grand, elle vérifie l'inégalité suivante :

$$\mathbb{E}\Big[d\big(A^n, g(B^n, Y^n)\big)\Big] \leq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] + \varepsilon \, .$$

La condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big]$ est donc suffisante pour atteindre un niveau de distorsion $D + \varepsilon$ à Bob.

3.7.3 Incertitude à Ève

En utilisant les particularités de la procédure d'encodage proposée ainsi que la contrainte (3.20), l'incertitude à Ève (moyennée sur l'ensemble des dictionnaires possibles) peut être bornée de la manière suivante :

$$H(A^n|E^n Z^n) \geq H(A^n|r_1) + H(r_f) + H(E^n|A^n) + H(Z^n|X^n) - H(E^n Z^n|r_1) - n\,\tfrac{\varepsilon}{4} \, . \quad (3.21)$$

Chaque terme du membre de droite de cette inégalité peut être étudié en utilisant les propriétés des séquences typiques, et en suivant les raisonnements de la section 2.3.3 et de [90, Section 2.3.*Step 3*] :

- Les mots de code $u^n(r_1)$ sont générés i.i.d. En suivant le raisonnement donné à la section 2.3.6 de la partie II, on peut montrer que, pour n suffisamment grand,
$$H(A^n|r_1) \geq n\left(H(A|U) - \tfrac{\varepsilon}{4}\right) \, .$$
- Comme la source aléatoire r_f est uniformément distribuée, de débit R_f,
$$H(r_f) = nR_f \, .$$
- Comme les sources sont i.i.d.,
$$H(E^n|A^n) = nH(E|A) \, .$$
- Comme le canal est sans mémoire et que l'entrée X^n est typique (voir [90, Eq. (2.46)]),
$$H(Z^n|X^n) \geq n\left(H(Z|X) - \tfrac{\varepsilon}{4}\right) \, .$$
- Comme $(u^n(r_1), E^n, Z^n)$ sont conjointement typiques, en suivant le raisonnement de [90, Eq. (2.54)], on peut montrer que
$$H(E^n Z^n|r_1) \leq n\left(H(EZ|U) + \tfrac{\varepsilon}{4}\right) \, .$$

En rassemblant les équations ci-dessus, on obtient l'inégalité suivante :

$$H(A^n|E^n Z^n) \geq n\Big(H(A|U) + R_f + H(E|A) + H(Z|X) - H(EZ|U) - \varepsilon\Big) \, ,$$

pour n suffisamment grand. Après quelques manipulations, et en utilisant les chaînes de Markov $U \multimap A \multimap E$ et $(U, E) \multimap X \multimap Z$, on montre que la condition suivante est suffisante pour atteindre l'incertitude $\Delta - \varepsilon$ à Ève :

$$\Delta \leq H(A|UE) - I(X; Z|UE) + R_f \, .$$

3.7.4 Fin de la démonstration

Les équations suivantes fournissent des conditions suffisantes pour l'atteignabilité du triplet $(k = 1, D, \Delta)$:

$$\begin{cases} R_1 > I(U;A) \\ R_2 > I(V;A|U) \\ R_f > 0 \\ R_1 < I(U;BY) \\ R_2 + R_f < I(V;BY|U) \\ R_2 + R_f < I(V;AZ|U) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V,B,Y))\big] \\ \Delta \leq H(A|UE) - I(X;Z|UE) + R_f \end{cases}$$

L'algorithme d'élimination de Fourier-Motzkin [156] conduit alors au système suivant :

$$\begin{cases} I(U;A) < I(U;BY) \\ I(V;A|U) < I(V;BY|U) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V,B,Y))\big] \\ \Delta < H(A|UE) - I(X;Z|UE) + I(V;BY|U) - I(V;A|U) \\ \Delta < H(A|UE) - I(X;Z|UE) + I(V;AZ|U) - I(V;A|U) \end{cases}$$

Cela démontre le théorème 3.8. □

3.8 Transmission d'une source binaire avec informations adjacentes CBE/CBS via un canal *wiretap* de type II (suite)

Dans cette section, nous reprenons l'exemple binaire de la section 3.5 et comparons un schéma hybride basé sur celui du théorème 3.8 avec ceux analysés à la section 3.5, à savoir le schéma numérique de la section 3.3 (voir la proposition 3.6) et un schéma purement analogique consistant à placer directement la soutce en entrée du canal (voir la proposition 3.7).

3.8.1 Codage hybride

Nous considérons le schéma hybride du théorème 3.8 avec les variables U, V et X définies de la manière suivante :

$$U = V \oplus W \,, \tag{3.22}$$

$$V \overset{\perp\!\!\!\perp A}{\sim} \mathcal{B}(\tfrac{1}{2}) \,, \tag{3.23}$$

$$X = V \oplus A \,, \tag{3.24}$$

ou $\oplus$ représente l'opérateur ou-exclusif binaire, W est indépendant de A et V, et $W \sim \mathcal{B}(u)$ pour $u \in [0\,;\frac{1}{2}]$.

3.8.2 Résultats numériques

La figure 3.11 représente l'incertitude maximale à Ève Δ en fonction de la probabilité d'effacement β (avec $\epsilon = 0.1$ et $\zeta = 0.1$.) pour

(*i*) la borne extérieure de la proposition 3.5,

(*ii*) le schéma hybride analogique/numérique du théorème 3.8 avec les variables (3.22)–(3.24) (et optimisation numérique de u),

(*iii*) le schéma numérique de la proposition 3.6 (avec optimisation numérique de u et q),

(*iv*) le schéma analogique de la proposition 3.7.

Si $\beta \leq 4\epsilon(1-\epsilon)$, B est moins bruité que E (voir la figure 3.8), et le schéma numérique est optimal (comme indiqué par la proposition 3.3), de même que le schéma hybride proposé. Ici, ce résultat semble également valable lorsque B est seulement « meilleur » que E, c.-à-d. pour $\beta \leq h_2(\epsilon)$.

Pour $\beta = 1$, comme indiqué à la section 3.5.3, le schéma analogique est meilleur que le schéma numérique. Conformément aux commentaires de la section 3.6.2.1, le schéma hybride proposé est toujours au moins aussi performant que ce schéma analogique.

Sur la figure 3.11, le schéma hybride analogique/numérique semble également être au moins aussi performant que le schéma numérique. Cependant, conformément aux commentaires de la section 3.6.2.2, et en fonction des paramètres ϵ, ζ, cela peut ne pas être le cas pour tout β dans $[h_2(\epsilon)\,;1[$.

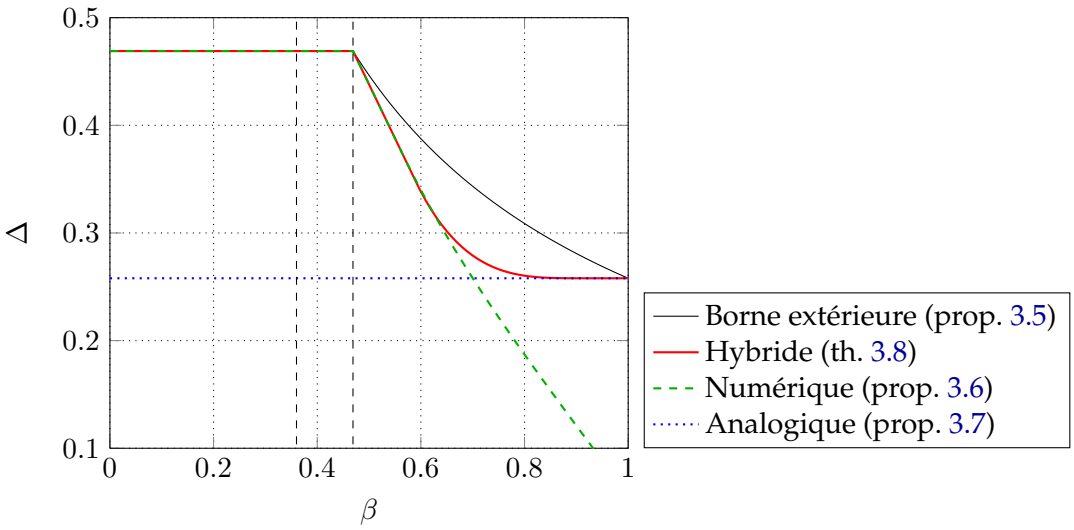


Figure 3.11 – Incertitude Δ en fonction de la probabilité d'effacement β ($\epsilon = 0.1$, $\zeta = 0.1$).

3.9 Transmission d'une source gaussienne via un canal *wiretap* gaussien

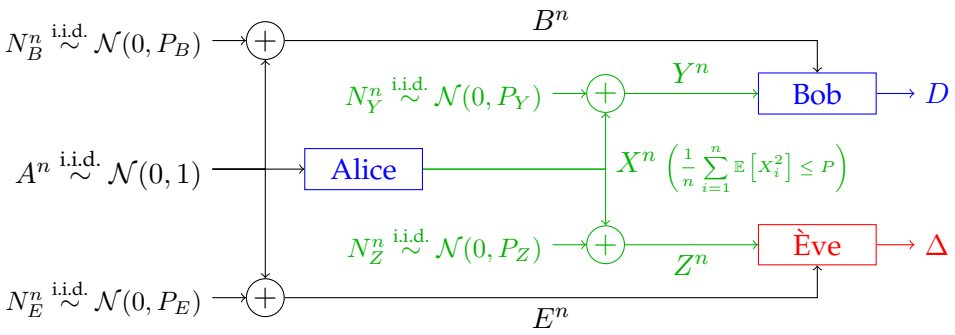


Figure 3.12 – Transmission d'une source gaussienne via un canal *wiretap* gaussien avec information adjacente aux récepteurs.

3.9.1 Modèle

Dans cette section, nous considérons la transmission d'une source gaussienne via un canal *wiretap* gaussien, avec une seule utilisation de canal par symbole de source (*matched-bandwidth*, $k = 1$). Plus précisément (voir la figure 3.12) : la source A est gaussienne centrée réduite ; les informations adjacentes à Bob et Ève sont produites à partir de A via des canaux indépendants à bruit blanc additif gaussien (BBAG) de puissances de bruit respectives P_B et P_E ; les canaux de communications d'Alice vers Bob et Ève sont des canaux BBAG indépendants de puissances de bruit respectives P_Y et P_Z. De plus, la puissance moyenne en entrée de ce canal est limitée à P. Une seule utilisation du canal est autorisée par symbole de source.

La distance euclidienne sur $\mathbb{R}$ est utilisée comme mesure de distorsion à Bob ($d(a,b) = (a-b)^2$, pour tous $a, b \in \mathbb{R}$). L'entropie différentielle $h(\cdot)$ permet de mesurer les incertitudes ; l'incertitude est alors un nombre réel quelconque ($\Delta \in \mathbb{R}$). Nous introduisons également la quantité $D_E = 2^{2\Delta}/(2\pi e)$, minorant de l'erreur quadratique moyenne de tout estimateur de A à Ève [31, Theorem 8.6.6].

Définition 3.3 (Atteignabilité)**.** Dans cette section, une paire $(D, D_E) \in {\mathbb{R}_+^*}^2$ est dite *atteignable* si, pour tout $\varepsilon > 0$, il existe un code (n, n), (F, g), tel que :

$$\begin{aligned} \mathbb{E}\left[\, \|A^n - g(B^n, Y^n)\|^2 \,\right] &\leq D + \varepsilon \,, \\ \frac{1}{n}\, h(A^n | E^n Z^n) &\geq \frac{1}{2} \log\left(2\pi e\, D_E\right) - \varepsilon \,, \\ \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}\left[X_i^2\right] &\leq P + \varepsilon \,, \end{aligned}$$

avec la sortie de l'encodeur placée en entrée du canal ($X^m = F(A^n)$).

	$P_B \leq P_E$	$P_B > P_E$
$P_Y < P_Z$	✓	?
$P_Y \geq P_Z$	✓	✓

Tableau 3.1 – Cas où $\mathcal{R}_{\text{num}}$ est optimale et où le principe de séparation est satisfait.

Bien que les théorèmes 3.1, 3.2, 3.8 soient énoncés et démontrés pour des alphabets finis, nous prenons la liberté de les appliquer dans cet exemple gaussien avec distorsion quadratique. Les distributions de probabilité des variables considérées doivent alors en plus vérifier la condition suivante :

$$\text{Var}\,[X] \leq P\,. \tag{3.25}$$

Les régions correspondantes sont notées avec un $\cdot^P$ supplémentaire ($\mathcal{R}_{\text{ext}}^P$, $\mathcal{R}_{\text{num}}^P$ and $\mathcal{R}_{\text{hyb}}^P$).

Notons que, comme les bruits sont gaussiens additifs, une des informations adjacentes (resp. un des canaux) est une version dégradée de l'autre. On peut identifier quatre cas en fonction des valeurs de P_B, P_E, P_Y et P_Z. D'après les résultats de la section 3.3.3, le principe de séparation est satisfait pour trois d'entre eux, comme indiqué dans le tableau 3.1. Le quatrième cas, où Bob a un meilleur canal ($P_Y < P_Z$) et une moins bonne information adjacente ($P_B > P_E$) que Ève, n'est pas résolu. Nous proposons dans cette section un schéma hybride analogique/numérique basé sur celui du théorème 3.8, optimal lorsque $P_Y < P_Z$ et $P_B \to \infty$.

3.9.2 Codage hybride

La proposition 3.9 ci-dessous est une conséquence du théorème 3.8 en choisissant les variables U, V et X de la manière suivante :

$$U = \emptyset\,, \tag{3.26}$$

$$V = \alpha A + \gamma N\,, \tag{3.27}$$

$$X = \big(\beta A - \gamma N\big)\sqrt{P}\,, \tag{3.28}$$

où $\alpha \in \mathbb{R}$, $\beta \in [0\,;1[$, $\gamma = \sqrt{1-\beta^2}$, et $N \sim \mathcal{N}(0,1)$ est une variable gaussienne centrée réduite indépendante de A. Notons que $X \sim \mathcal{N}(0,P)$ est une fonction déterministe de A et V:

$$X = \big((\alpha+\beta)A - V\big)\sqrt{P}\,. \tag{3.29}$$

La fonction $\hat{A}$ est définie comme l'estimateur à EQM minimale de A à partir de (V,B,Y).

Le schéma hybride analogique/numérique de la section 3.6 avec les variables (3.26)–(3.28) est représenté à la figure 3.13.

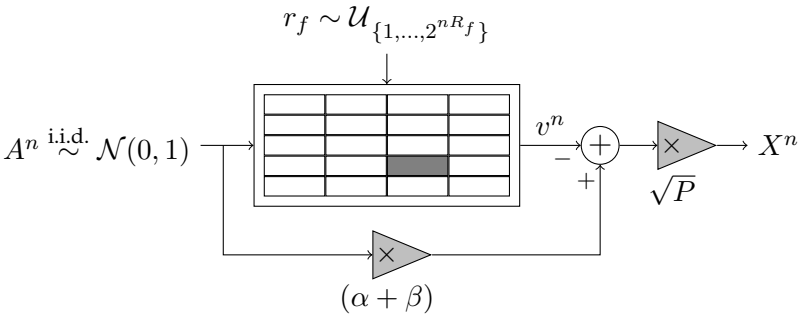


Figure 3.13 – Schéma hybride analogique/numérique pour la transmission sécurisée d'une source gaussienne via un canal *wiretap* gaussien.

Proposition 3.9 (Schéma hybride). *Une paire* $(D, D_E) \in {\mathbb{R}_+^*}^2$ *est atteignable si*

$$D \geq \frac{1}{1+\frac{1}{P_B}+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2}\,, \tag{3.30}$$

$$D_E \leq \frac{1}{1+\frac{1}{P_E}+\frac{P}{P_Z}\left(1+\frac{\gamma^2}{P_E}\right)} \cdot \min\left\{\frac{1+\frac{1}{P_B}+\frac{P}{P_Y}\left(1+\frac{\gamma^2}{P_B}\right)}{1+\frac{1}{P_B}+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2}\,;1+\gamma^2\,\frac{P}{P_Z}\right\}\,, \tag{3.31}$$

pour $\alpha \in \mathbb{R}$, $\beta \in [0\,;1[$ *tels que*

$$\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2 \leq \frac{P}{P_Y}\left(1+\frac{\gamma^2}{P_B}\right)\,, \tag{3.32}$$

où

$$\gamma = \sqrt{1-\beta^2}\,. \tag{3.33}$$

Démonstration. Voir l'annexe E.4. □

Remarque 3.3. Dans le schéma proposé, contrairement au *dirty-paper coding* pour les communications point-à-point sans contrainte de sécurité [30], la source A (vue comme l'état d'un canal, connu à l'émetteur – voir la figure 3.9) et l'entrée du canal X ne sont pas indépendantes.

3.9.3 Cas particulier : $P_Y < P_Z$, $P_B \to \infty$

Nous nous concentrons à présent sur le cas non résolu représenté par « **?** » dans le tableau 3.1. En particulier, nous supposons que $P_Y < P_Z$. Alors, si Bob n'a pas d'information adjacente ($B = \emptyset$, ou de manière équivalente $P_B \to \infty$) :

- Le schéma hybride analogique/numérique de la proposition 3.9 est optimal (voir le théorème 3.10).
- Le schéma numérique du théorème 3.2 est strictement sous-optimal (voir la proposition 3.11 et la figure 3.14.

Théorème 3.10 (Caractérisation optimale). *Si $P_Y < P_Z$ et $B = \emptyset$, $(D, D_E) \in {\mathbb{R}_+^*}^2$ est atteignable si et seulement si*

$$D \geq \frac{1}{1+\frac{P}{P_Y}}\,, \tag{3.34}$$

$$D_E \leq \frac{1}{\max\left\{1\,;\,\frac{1}{D}\cdot\frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}\right\}+\frac{1}{P_E}}\,. \tag{3.35}$$

Démonstration. La réciproque est démontrée en annexe E.5.

Le sens direct est une conséquence de la proposition 3.9, en faisant tendre P_B vers l'infini et en choisissant, pour tout $D \in \left[\frac{1}{1+\frac{P}{P_Y}}\,;\,\frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}\right[$:

$$\alpha = \frac{\beta+\gamma^2\sqrt{\frac{1}{D}\left(\frac{P}{P_Y}-\frac{P}{P_Z}\right)}}{1+\gamma^2\frac{P}{P_Y}} - \beta\,, \tag{3.36}$$

$$\beta = \sqrt{\frac{P_Z}{P}}\sqrt{1+\frac{P}{P_Z}-D\left(1+\frac{P}{P_Y}\right)}\,. \tag{3.37}$$

Les détails sont donnés en annexe E.6. □

La proposition suivante donne une expression simple de la région $\mathcal{R}_{\text{num}}^P$ (atteignable par le schéma numérique de la section 3.3).

Proposition 3.11 (Schéma numérique). *Si $P_Y < P_Z$ et $B = \emptyset$, $(D, D_E) \in \mathcal{R}_{num}^P$ si et seulement si il existe $\mu \in \left[\frac{1}{1+\frac{P}{P_Y}}\,;1\right]$ tel que*

$$D \geq \frac{1}{1+\frac{P}{P_Y}}\,, \tag{3.38}$$

$$D_E \leq \frac{1}{\frac{1}{\mu}+\frac{1}{P_E}}\cdot\min\left\{1\,;\,\frac{D\left(1+\frac{P}{P_Y}\right)}{1+\mu\frac{P}{P_Z}-(1-\mu)\frac{P_Y}{P_Z}}\right\}\,. \tag{3.39}$$

Démonstration. La réciproque est démontrée en annexe E.7, de la même manière que celle du théorème 3.10.

Le sens direct est une conséquence du théorème 3.2 avec des variables U, V, Q et $T = X$ gaussiennes. Les détails sont omis. □

Remarque 3.4. Si $D \geq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$, alors $\mu = 1$ est optimal dans la proposition 3.11, donnant les inégalités (3.34), (3.35) du théorème 3.10. Le schéma numérique de la section 3.3 est donc optimal dans cette zone. Pour de tels niveaux de distorsion, la quantité $D_E = \frac{1}{1+\frac{1}{P_E}} = \text{Var}\,[A|E]$ est atteignable, indiquant que Ève ne peut obtenir aucune information de la communication entre Alice et Bob.

Nous comparons également les deux schémas ci-dessus avec un schéma purement analogique, consistant à placer une version amplifiée de la source en entrée du canal. Ses performances sont données par la proposition suivante.

Proposition 3.12 (Schéma analogique). *Si $B = \emptyset$, $(D, D_E) \in {\mathbb{R}_+^*}^2$ est atteignable si*

$$D \geq \frac{1}{1 + \frac{P}{P_Y}} ,$$
$$D_E \leq \frac{1}{1 + \frac{1}{P_E} + \left[\left(\frac{1}{D} - 1\right) \frac{P_Y}{P_Z}\right]_+} .$$

Démonstration. Voir l'annexe E.8. □

Remarque 3.5. Si $D = D_{\min} \triangleq \frac{1}{1+\frac{P}{P_Y}}$, les inégalités de la proposition 3.12 deviennent celles du théorème 3.10 : le schéma analogique est optimal.

Remarque 3.6. Lorsqu'il n'y a pas de contrainte de sécurité ($D_E = 0$), les trois schémas considérés dans cette section sont équivalents et atteignent la distorsion $D_{\min}$ [47, 52].

Résultats numériques

La figure 3.14 représente l'incertitude maximale D_E en fonction du niveau de distorsion D (avec $P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$) pour

(*i*) le schéma hybride analogique/numérique optimal du théorème 3.10,

(*ii*) le schéma numérique de la proposition 3.11 (avec optimisation numérique de μ),

(*iii*) le schéma analogique de la proposition 3.12.

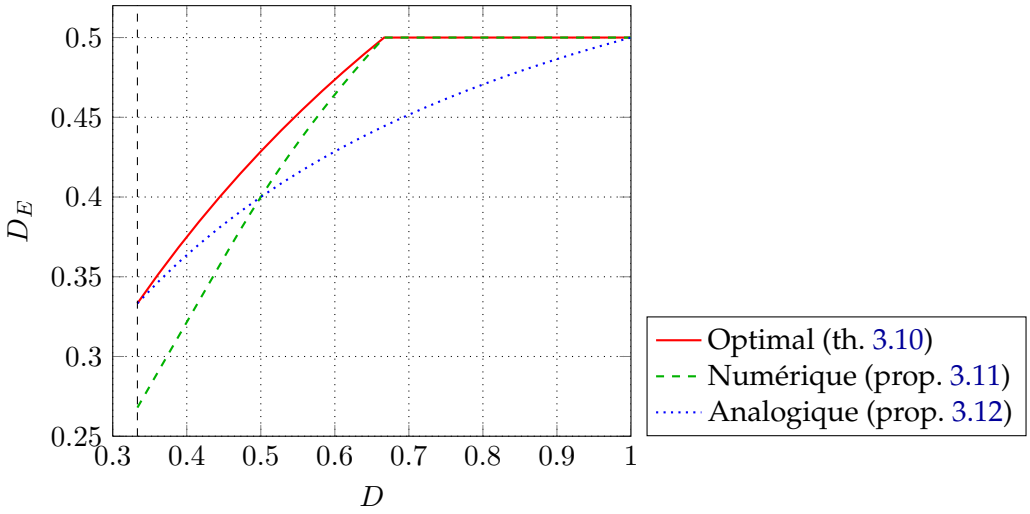


Figure 3.14 – Quantité D_E en fonction de D ($P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$).

De fait, le schéma hybride analogique/numérique proposé est meilleur que les deux autres. De plus, alors que le schéma numérique est optimal pour $D \geq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$ (voir la remarque 3.4) et que le schéma analogique l'est pour $D = D_{\min}$ (voir la remarque 3.5), une combinaison (*time-sharing*) de ceux-ci est insuffisante pour atteindre la région toute entière (voir la figure 3.14 et le théorème 3.10.

3.10 Conclusion

Dans ce chapitre, nous avons étudié le problème général du codage de source-canal pour la transmission sécurisée d'une source via un canal bruité, avec information adjacente aux récepteurs. Il peut être vu comme la généralisation des problèmes de codage de source sous contrainte de sécurité avec information adjacente (étudié à la section 2.4), et du canal *wiretap*. Une borne extérieure générale pour la région débit-distorsion-incertitude correspondante a été démontrée, ainsi que deux bornes intérieures basées sur (*i*) un schéma purement numérique qui combine le codage de source sécurisé du chapitre 2 et le codage pour les canaux de diffusion avec messages confidentiels [32], et (*ii*) un nouveau schéma hybride analogique/numérique (dans le cas *matched-bandwidth*).

Les bornes proposées sont disjointes dans le cas général, mais, sous certaines conditions, le schéma numérique est optimal. Un contre-exemple simple montre cependant qu'une stratégie *conjointe* de codage source-canal peut faire mieux dans d'autres cas. À première vue, cela n'est pas surprenant : il est bien connu que le codage/décodage conjoint est adapté aux canaux de diffusion [155], lorsque tous les récepteurs doivent parfaitement reconstruire la source. Mais le problème avec contrainte de *sécurité* est tout à fait différent : Alice souhaite aider seulement un récepteur (Bob) tout en trompant le second (Ève). L'intuition indique donc plutôt qu'il faudrait faire le contraire, à savoir séparer les opérations de codage de source et de codage de canal, comme dans les propositions 3.3 et 3.4.

D'autre part, le schéma hybride analogique/numérique proposé peut être utile en termes de sécurité. Dans un cas gaussien quadratique, avec information adjacente au seul adversaire, cette stratégie se révèle optimale. Nous n'avons pas réussi à montrer un tel résultat dans le cas plus général où les deux récepteurs disposent d'information adjacente. Un schéma plus évolué est nécessaire. La superposition des deux schémas numérique et hybride (comme dans [161] lorsqu'il n'y a pas de contrainte de sécurité) pourrait être utile. Notons qu'alors l'incertitude à Ève semble relativement difficile à analyser.

CHAPITRE 4

Quantification vectorielle haute-résolution pour la détection de processus corrélés

Résumé. Ce chapitre traite de l'effet de la quantification sur les performances du test de Neyman-Pearson. On suppose qu'un capteur observe des échantillons d'un processus multivarié stationnaire ergodique. Chaque échantillon est traité par un quantificateur à N points, puis transmis à un centre de décision qui réalise alors un test d'hypothèse. Pour tout niveau de fausse alarme, il est montré que la probabilité de manque du test de Neyman-Pearson converge exponentiellement vers zéro quand le nombre d'échantillons tend vers l'infini, si le processus observé satisfait certaines conditions de mélangeance. La principale contribution de ce chapitre est de donner une expression compacte de l'exposant d'erreur dans le régime des hautes résolutions, c'est-à-dire quand le nombre N de points de quantification tend vers l'infini, généralisant les résultats de Gupta et Hero au cas d'observations non-indépendantes. Si d représente la dimension de chaque échantillon, il est montré que l'exposant d'erreur converge à la vitesse $N^{2/d}$ vers celui obtenu sans quantification. À partir de ce résultat, des stratégies de quantification donnant des exposants d'erreur élevés sont déterminées. Les résultats numériques indiquent que celles-ci peuvent effectivement améliorer les performances en termes d'erreur de détection.

4.1 Introduction

Considérons un capteur qui transmet une séquence de mesures à un centre de décision (CD) dont la mission est de détecter un signal donné. Par exemple, une caméra de surveillance envoie des images à un contrôleur distant qui souhaite pouvoir détecter certains objets dans la région concernée. Cette situation apparaît également dans le contexte des réseaux de capteurs sans fil (RCSF) où un centre de fusion collecte les mesures d'un grand nombre de capteurs, et les analyse dans le but de détecter des événements anormaux [5,25]. Dans ces applications, des contraintes (en termes de bande passante, délai et capacités de stockage) limitent les débits de transmission. Les mesures doivent donc être quantifiées (compressées) avant envoi. De fait, cette étape de quantification peut sévèrement dégrader les performances de détection du système. Dans ce chapitre, nous considérons qu'un test d'hypothèse est réalisé au CD. Les données disponibles correspondent à une version quantifiée d'un processus multivarié stationnaire ergodique à temps dis-

cret. Notre but est d'analyser l'impact d'un quantificateur donné sur la détection, et de caractériser ceux qui garantissent de bonnes performances au CD.

Ces dernières décennies, de nombreux travaux ont été dédiés à la recherche de stratégies de quantification performantes et à leur mise en œuvre pratique [54]. Le critère le plus populaire pour la sélection des quantificateurs est l'erreur quadratique moyenne (EQM) entre le signal quantifié et la source originale [50]. Une caractérisation analytique des quantificateurs minimisant l'EQM est difficile dans le cas général. Bennett [8] a introduit l'étude de la quantification *haute-résolution* pour la reconstruction des signaux scalaires. L'idée est d'analyser l'EQM dans le régime asymptotique où le nombre de niveaux de quantification tend vers l'infini. Dans ce cas, on peut obtenir une expression explicite de l'EQM, ainsi qu'une caractérisation des familles de quantificateurs qui minimisent cette EQM asymptotique. Cette approche haute-résolution a été par la suite étendue aux observations vectorielles [111]. Cependant, le critère de l'EQM est pertinent lorsque le but du CD est de reconstruire la source ; il peut être tout à fait inapproprié pour d'autres applications. Pour cette raison, de nombreuses mesures de distorsion ont été proposées pour la quantification *ciblée*, adaptée à une certaine tâche, comme l'estimation de paramètres [108, 129, 167], la détection [61, 74, 128, 130, 149, 153, 154], ou la classification [125] (voir également [64]). En particulier, la recherche de règles de quantification optimales pour les tests d'hypothèse a été l'objet d'une grande attention. Poor et Thomas [130] ont utilisé les distances de Ali-Silvey entre densités. Poor [129] a ensuite proposé la f-divergence généralisée et étudié son comportement dans le régime des hautes résolutions. Picinbono et Duvaut [128] ont considéré un critère de déviation, et monté que la procédure optimale correspondante revient à une simple quantification scalaire du rapport de vraisemblance. Tsitsiklis [154] a étudié les propriétés de ces quantificateurs par rapport à diverses mesures de distorsion. Plus récemment, à la suite des travaux de Tenney et Sandell [149], Tsitsiklis [153], et Benitz et Bucklew [7], Gupta et Hero [61] ont étudié la sélection des quantificateurs haute-résolution pour les tests d'hypothèse. Dans ces travaux, le centre de décision rassemble les réalisations de n variables indépendantes et identiquement distribuées (i.i.d.), chacune étant préalablement traitée par un quantificateur fixé. La densité de probabilité de ces échantillons est supposée connue sous les deux hypothèses. La procédure de Neyman-Pearson (NP) constitue dans ce cas un test uniformément plus puissant. Celle-ci consiste à rejeter l'hypothèse nulle quand le logarithme du rapport de vraisemblance (LRV) est supérieur à un certain seuil [87]. Ce seuil est habituellement choisi de sorte que la probabilité de fausse alarme du test (c'est-à-dire, la probabilité de rejeter l'hypothèse nulle alors que celle-ci est vraie, encore appelée risque de première espèce) est fixée à un certain niveau α. Les performances du test NP de niveau α peuvent être évaluées en termes de probabilité de manque (la probabilité d'accepter l'hypothèse nulle alors qu'elle est fausse, également appelée risque de deuxième espèce). Dans notre cas, cette probabilité de manque dépend évidemment du quantificateur utilisé par le capteur ; une approche naturelle serait donc de sélectionner celui qui la minimise. Malheureusement, celle-ci n'admet aucune expression simple, et l'effet du quantificateur n'est pas directement mesurable. Afin de lever cette difficulté, on peut

étudier son comportement dans le cas où le nombre n d'échantillons tend vers l'infini. Si les observations sont i.i.d., le lemme de Stein [31] indique que la probabilité de manque tend exponentiellement vers zéro. Il peut être alors judicieux de sélectionner les quantificateurs qui maximisent le taux de convergence correspondant (appelé *exposant d'erreur*). Cependant, cette maximisation n'est pas réalisable en pratique : le quantificateur intervient dans l'exposant d'erreur de manière bien trop complexe, et un trop grand nombre de paramètres est nécessaire pour le caractériser. En suivant l'idée de [8, 111], Gupta et Hero se sont concentrés sur le régime des hautes résolutions pour obtenir une expression compacte de la perte en exposant d'erreur introduite par la quantification.

La plupart des travaux précités considèrent des observations indépendantes. Cependant, la détection de processus corrélés est une question cruciale dans de nombreux contextes [24, 62, 144, 160]. Chamberland et Veeravalli [24] ont analysé l'impact de la densité des capteurs dans un RCSF sur la détection, quand les observations sont corrélées. Willett et al. [160] ont étudié la quantification binaire (sur un seul bit) d'une paire de variables aléatoires gaussiennes. Dans le cas de la détection d'un signal gaussien markovien dans du bruit, Sung et al. [144] ont démontré que, pour un niveau de fausse alarme fixé, la probabilité du test NP converge exponentiellement vers zéro, et fourni une expression explicite de l'exposant d'erreur. Hachem et al. [62] ont par la suite étendu ces résultats aux processus de diffusion gaussiens échantillonnés de manière irrégulière. Notons cependant que, dans les travaux précédents [62, 144], le CD a directement accès aux observations du capteur ; la problématique de la quantification n'y est pas abordée.

Dans ce chapitre, nous étudions les performances du test de Neyman-Pearson réalisé sur une version quantifiée d'un processus multivarié stationnaire ergodique. Nous généralisons les travaux de Gupta et Hero [61] au cas où les observations ne sont pas i.i.d. (sous l'hypothèse nulle, sous l'alternative, ou sous les deux hypothèses). Dans cette situation, le lemme de Stein ne s'applique pas. L'exposant d'erreur n'admet pas d'expression explicite, et la détermination de quantificateurs efficaces est plus difficile. À condition que le processus satisfasse certaines propriétés d'oubli (les observations au temps présent doivent devenir quasi indépendantes des observations passées après un certain temps), nous démontrons que la probabilité de manque du test NP de niveau α tend exponentiellement vers zéro, lorsque le nombre d'observations tend vers l'infini. Notre principale contribution est une expression compacte de l'exposant d'erreur dans le régime des hautes résolutions. Si N est le nombre de points de quantification (ou de manière équivalente, si chaque observation est quantifiée sur $\log_2(N)$ bits), nous montrons que l'exposant d'erreur converge, lorsque N tend vers l'infini, vers l'exposant d'erreur idéal qu'on obtiendrait si les observations (non-quantifiées) étaient directement accessibles au CD. Plus précisément, nous montrons que la perte en exposant d'erreur tend vers zéro à la vitesse $N^{-2/d}$, où d représente la dimension de chaque observation. L'exposant d'erreur asymptotique dépend des distributions de probabilité du processus sous les deux hypothèses. Il dépend également de la stratégie de quantification via sa *densité limite* et son *profil limite*. La densité limite peut être interprétée comme le nombre asymptotique de cellules dans le voisinage de chaque point de l'espace d'observation. Le profil

limite contient des informations sur la forme de ces cellules. Par conséquent, la sélection de quantificateurs haute-résolution adaptés se résume à la détermination des densités et profils limites qui minimisent la perte asymptotique en exposant d'erreur. Pour des observations scalaires ($d = 1$), notre expression compacte donne une caractérisation immédiate des quantificateurs haute-résolution optimaux. Dans le cas vectoriel ($d \geq 2$), en suivant l'approche de [61], nous pouvons seulement maximiser l'exposant d'erreur dans certaines classes de quantificateurs. Notons que ces résultats sont valables sous l'hypothèse que le processus observé « oublie » les observations passées suffisamment vite. Nous démontrons que celle-ci est en particulier vérifiée par une large classe de modèles de Markov cachés. Quelques exemples numériques sont donnés, par exemple dans le cas où les observations correspondent à un signal modulé dans le plan en-phase/quadrature.

La suite de ce chapitre est organisée de la manière suivante. Dans la section 4.2, nous décrivons le modèle d'observation. Nous rappelons également quelques résultats connus sur les tests de Neyman-Pearson, et donnons l'exposant d'erreur associé, lorsque le CD a un accès direct aux observations (non-quantifiées). Le cadre de la quantification vectorielle est introduit à la section 4.3. L'impact d'une telle quantification sur l'exposant d'erreur est évalué dans le régime des hautes résolutions à la section 4.4. Nous déterminons des stratégies de quantification qui permettent de réduite cette dégradation. La section 4.5 est consacrée à la démonstration du résultat principal. Dans la section 4.6, nous donnons des conditions suffisantes sur les noyaux de transition et d'observation de processus de Markov cachés garantissant que nos résultats s'appliquent. La section 4.7 est dédiée aux illustrations numériques. La section 4.8 conclut le chapitre.

Notations

Pour toute suite $(y_i)_{i\in\mathbb{Z}}$ et tout entier $k \leq \ell$, $y_{k:\ell}$ désigne le vecteur $(y_k, y_{k+1}, \ldots, y_\ell)$; la notation $y_{\mathbb{Z}}$ est utilisée pour désigner la suite toute entière. Si y est un vecteur de dimension d, on note $y^{(i)}$ sa $i^{\text{ème}}$ composant et $\|y\|$ sa norme euclidienne. On note $\|A\|$ la norme spectrale de toute matrice carrée A. La notation $.^{\mathrm{T}}$ désigne l'opérateur de transposition.
Une fonction à valeurs réelles $f\colon y_{k:\ell} \mapsto f(y_{k:\ell})$ sur $\mathsf{S} \subset \mathbb{R}^d \times \cdots \times \mathbb{R}^d$ est dite de classe C_3 sur S si elle est trois fois continûment différentiable sur S. On note $\nabla_{y_m} f(y_{k:\ell})$ son gradient par rapport à y_m au point $y_{k:\ell}$. Lorsqu'aucune variable n'est spécifiée, $\nabla g(y)$ désigne simplement le gradient (de dimension d) de la fonction réelle $y \mapsto g(y)$ définie sur $\mathsf{Y} \subset \mathbb{R}^d$. La matrice hessienne de f est définie par $\left[\nabla^2_{y_m,y_n} f\right]_{i,j} = \frac{\partial^2 f}{\partial y_m^{(i)}\, \partial y_n^{(j)}}$ pour tous $i, j \in \{1, \ldots, d\}$. De plus, $\nabla^2_{y_m}$ désigne simplement $\nabla^2_{y_m,y_m}$.
La tribu borélienne sur X est notée $B(\mathsf{X})$. La sous-algèbre de $B(\mathsf{Y}^{\mathbb{Z}})$ associée au vecteur aléatoire $Y_{1:n}$ est notée $\sigma(Y_{1:n})$. La convergence en probabilité (resp. en norme L^r pour la probabilité $\mathbb{P}_0$) quand $n \to \infty$ est notée $\xrightarrow[n\to\infty]{P}$ (resp. $\xrightarrow[n\to\infty]{L^r(\mathbb{P}_0)}$).
Le logarithme naturel est noté $\log(\cdot)$. L'opérateur de composition, $\circ$: pour toutes fonctions f, g, $f \circ g(x) = f(g(x))$. La notation petit-o, $o_N(\cdot)$, est utilisée pour désigner un terme négligeable quand N tend vers l'infini.

4.2 Test de Neyman-Pearson avec accès direct aux observations

4.2.1 Modèle d'observation

Considérons deux mesures de probabilité $\mathbb{P}_0$ et $\mathbb{P}_1$ sur un espace de probabilité approprié. Soit $(Y_k)_{k\in\mathbb{Z}}$ un processus stationnaire ergodique pour $\mathbb{P}_0$ et $\mathbb{P}_1$, à valeurs dans un sous-ensemble borné convexe Y de $\mathbb{R}^d$. On associe une hypothèse ($\mathsf{H}0$ et $\mathsf{H}1$ respectivement) à chacune des probabilités $\mathbb{P}_0$ et $\mathbb{P}_1$, et étudions le problème de la détection de $\mathsf{H}1$ contre $\mathsf{H}0$ à partir d'un ensemble de n observations $Y_{1:n} = (Y_1, \dots, Y_n)$.

Pour tout $i \in \{0, 1\}$, on suppose que $\mathbb{P}_i$ est la distribution de probabilité du processus $(Y_k)_{k\in\mathbb{Z}}$ sur l'espace canonique $(\mathsf{Y}^{\mathbb{Z}}, B(\mathsf{Y}^{\mathbb{Z}}))$. On note $P_{i,n}$ la restriction de $\mathbb{P}_i$ à $\sigma(Y_{1:n})$, et $\mathbb{E}_0$ (resp. $\mathbb{E}_1$) l'espérance associée à $\mathbb{P}_0$ (resp. $\mathbb{P}_1$). On introduit également la mesure de référence μ, égale à la mesure de Lebesgue restreinte à Y.

Hypothèse 4.1 (Densités)**.** Les propriétés suivantes sont vraies pour tout $i \in \{0, 1\}$.

1. Pour tout $n \geq 1$, $P_{i,n}$ admet une densité p_i par rapport à $\mu^{\otimes n}$.
2. $p_i(y_{1:n}) > 0$ pour tout $y_{1:n} \in \mathsf{Y}^n$.
3. $\mathbb{E}_0 \left|\log p_i(Y_0)\right| < \infty$.

La densité p_i de $P_{i,n}$ dépend évidemment de n, mais nous supprimons l'indice n pour simplifier les notations. Pour tout $i \in \{0, 1\}$, on définit $p_i(y_n|y_{1:n-1}) = p_i(y_{1:n})/p_i(y_{1:n-1})$ avec la convention $p_i(y_n|y_{1:n-1}) = p_i(y_n)$ si $n = 1$. L'hypothèse 4.1.2 implique que les distributions $P_{0,n}$ et $P_{1,n}$ sont absolument continues l'une par rapport à l'autre.

4.2.2 Test du rapport de vraisemblance

Nous étudions à présent la détection de $\mathsf{H}1$ contre $\mathsf{H}0$ à partir de l'observation directe de n mesures $Y_{1:n}$. Le logarithme du rapport de vraisemblance (LRV) s'écrit

$$L_n = \log \frac{p_1(Y_{1:n})}{p_0(Y_{1:n})} \,. \tag{4.1}$$

Le test NP rejette l'hypothèse nulle $\mathsf{H}0$ quand L_n est supérieur à un certain seuil γ. Pour tout $\alpha \in]0\,;1[$, la probabilité de manque du test NP de niveau α est définie par

$$\beta_n(\alpha) = \inf \mathbb{P}_1 \left[L_n < \gamma\right] \,,$$

où l'infimum est pris sur l'ensemble des γ tels que la probabilité de fausse alarme n'excède pas α :

$$\gamma \text{ t.q. } \mathbb{P}_0 \left[L_n > \gamma\right] \leq \alpha \,.$$

Pour tout $n \geq 1$ et tout $\alpha \in]0\,;1[$, le lemme de Neyman-Pearson indique que $\beta_n(\alpha)$ est la probabilité de manque minimale parmi tous les tests binaires de niveau α basés sur l'observation de $Y_{1:n}$. La quantité $\beta_n(\alpha)$ est une métrique-clé pour l'étude des performances

des tests d'hypothèse. Malheureusement, il n'admet en général aucune expression explicite simple. Dans la suite, nous étudions le comportement asymptotique de $\beta_n(\alpha)$ lorsque le nombre d'observations n tend vers l'infini. Dans ce régime, on peut montrer que, sous certaines hypothèses,

$$\beta_n(\alpha) \simeq \exp(-n\,K) \tag{4.2}$$

où K est une constante appelée *exposant d'erreur*.

4.2.3 Exposant d'erreur

L'évaluation de l'exposant d'erreur K dans (4.2) est basée sur le lemme suivant [27].

Lemme 4.1 ([27]). *Supposons qu'un test binaire est réalisé sur la suite de variables aléatoires $\check{Y}_{1:n} = (\check{Y}_1, \ldots, \check{Y}_n)$. Notons $\check{p}_0$ (resp. $\check{p}_1$) la densité de $\check{Y}_{1:n}$ sous* H0 *(resp.* H1*), par rapport à une mesure de référence quelconque. Supposons alors que, sous* H0*,*

$$\frac{1}{n} \log \frac{\check{p}_0(\check{Y}_{1:n})}{\check{p}_1(\check{Y}_{1:n})} \xrightarrow[n\to\infty]{P} \kappa$$

où κ est une constante (déterministe) telle que $0 < \kappa \leq \infty$. Alors, pour tout $\alpha \in]0\,;1[$, la probabilité de manque $\beta_n(\alpha)$ du test de Neyman-Pearson de niveau α vérifie la propriété suivante :

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n(\alpha) = -\kappa\ .$$

Le lemme 4.1 indique que l'exposant d'erreur, s'il existe, coïncide avec la limite en probabilité (sous $\mathbb{P}_0$) de $-(1/n)L_n$, où L_n est le LRV (4.1). L'existence de l'exposant d'erreur est une conséquence directe de l'hypothèse suivante.

Hypothèse 4.2 (Convergence). Pour tout $i \in \{0,1\}$, $(\log p_i(Y_0|Y_{-m:-1}))_{m\geq 0}$ est une suite convergente de $L^1(\mathbb{P}_0)$.

Nous pouvons à présent étudier la limite du LRV L_n et démontrer le résultat suivant, qui donne la forme générale de l'exposant d'erreur.

Théorème 4.2 (Exposant d'erreur). *Sous les hypothèses 4.1 et 4.2,*

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n(\alpha) = -K\ ,$$

où K est la constante définie par

$$K = \lim_{m\to\infty} \mathbb{E}_0 \left[\log \frac{p_0}{p_1}(Y_0|Y_{-m:-1}) \right]\ . \tag{4.3}$$

Démonstration. Le résultat est une conséquence de la règle de chaîne, de l'inégalité triangulaire, et de la stationnarité du processus $(Y_k)_{k\in\mathbb{Z}}$ sous $\mathbb{P}_0$. Voir la partie II pour de plus amples détails. □

Remarque 4.1. L'hypothèse 4.1 est une extension de celle faite par Gupta et Hero [61, Section III, pp.1956]. L'hypothèse 4.2 n'apparaît pas dans [61] ; elle est vérifiée par les processus i.i.d. (dans ce cas, le théorème 4.2 est connu sous le nom de lemme de Stein). L'hypothèse 4.2 est satisfaite par les processus à faible dépendance (m-dependants), tels que les processus à moyenne mobile [20]. Dans ce cas, l'observation actuelle Y_0 est indépendante des observations passées $Y_{-m-1}, Y_{-m-2}, \ldots$ dès que m est suffisamment grand. La section 4.6 décrit une large classe de modèles de Markov cachés pour lesquels l'hypothèse 4.2 est vérifiée.

4.3 Quantification

4.3.1 Définitions

Soit $N \geq 2$ un entier fixé. Un quantificateur à N points est un triplet $(\mathcal{C}_N, \Xi_N, \xi_N)$ où

- $\mathcal{C}_N = \{C_{N,1}, \ldots, C_{N,N}\}$ est un ensemble de N *cellules* (boréliens de Y de volume non-nul) qui partitionnent Y ;
- $\Xi_N = \{\xi_{N,1}, \ldots, \xi_{N,N}\}$ est un ensemble arbitraire de N éléments distincts ; et
- $\xi_N : \mathsf{Y} \to \Xi_N$ est une fonction telle que $\xi_N(y) = \xi_{N,j}$ si $y \in C_{N,j}$.

Pour tous N, k, on note

$$Z_{N,k} = \xi_N(Y_k)$$

la $k^{\text{ème}}$ observation quantifiée sur $\log_2(N)$ bits. On suppose que le quantificateur $(\mathcal{C}_N, \Xi_N, \xi_N)$ est connu du centre de décision. Le but est à présent de décider entre les hypothèses $\mathsf{H0}$ et $\mathsf{H1}$ à partir de $Z_{N,1:n}$.

4.3.2 Exposant d'erreur avec observations quantifiées

Pour un nombre d'observations n fixé, le LRV des observations quantifiées est défini par

$$L_{N,n} = \log \frac{p_{1,N}\left(Z_{N,1:n}\right)}{p_{0,N}\left(Z_{N,1:n}\right)} ,$$

où, pour tout $i \in \{0,1\}$, et tous $\xi_{N,j_{1:n}} = (\xi_{N,j_1}, \ldots, \xi_{N,j_n}) \in \Xi_N^n$,

$$p_{i,N}(\xi_{N,j_{1:n}}) = P_{i,n}(C_{N,j_1} \times \cdots \times C_{N,j_n})$$

est la probabilité que les observations $Y_1, \ldots, Y_n$ tombent respectivement dans les cellules $C_{N,j_1}, \ldots, C_{N,j_n}$ associées aux points $\xi_{N,j_1}, \ldots, \xi_{N,j_n}$. On définit également la probabilité conditionnelle suivante :

$$p_{i,N}(\xi_{N,j_n} | \xi_{N,j_{1:n-1}}) = \frac{p_{i,N}(\xi_{N,j_{1:n}})}{p_{i,N}(\xi_{N,j_{1:n-1}})} .$$

Pour tout $\alpha \in]0\,;1[$, on note $\beta_{N,n}(\alpha)$ la probabilité de manque du test NP de niveau α réalisé sur les observations quantifiées, c'est-à-dire l'infimum de $\mathbb{P}_1\left[L_{N,n} < \gamma\right]$ sur tous

les γ t.q. $\mathbb{P}_0\left[L_{N,n} > \gamma\right] \leq \alpha$. L'exposant d'erreur associé à $\beta_{N,n}(\alpha)$ est donné par le résultat suivant (similaire au théorème 4.2).

Corollaire 4.3 (Exposant d'erreur avec observations quantifiées)**.** *Soit $N \geq 2$ fixé. Si l'hypothèse 4.1 est vérifiée, et si $(\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1}))_{m\geq 0}$ est une suite convergente de $L^1(\mathbb{P}_0)$ pour tout $i \in \{0,1\}$, alors*

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_{N,n}(\alpha) = -K_N \ ,$$

où K_N est la constante définie par

$$K_N = \lim_{m\to\infty} \mathbb{E}_0 \left[\log \frac{p_{0,N}}{p_{1,N}}(Z_{N,0}|Z_{N,-m:-1}) \right] \ . \tag{4.4}$$

Ce résultat donne l'exposant d'erreur K_N associé au test NP réalisé sur les observations quantifiées. Une question naturelle est la suivante : comment le choix du quantificateur affecte-t-il cet exposant d'erreur ? Malheureusement, l'expression ci-dessus ne permet d'évaluer directement cet impact. Dans la suite, nous adoptons l'approche de [61,111] et nous concentrons sur le cas où le nombre de points N tend vers l'infini (quantificateurs à *haute résolution*). Nous démontrons alors une expression asymptotique simple de K_N. En particulier, si le processus $(Y_k)_{k\in\mathbb{Z}}$ et la suite de quantificateurs $(\mathcal{C}_N, \Xi_N, \xi_N)_{N\geq 1}$ vérifient certaines hypothèses, cet exposant d'erreur K_N converge vers K quand N tend vers l'infini.

4.4 Performances des quantificateurs haute-résolution

4.4.1 Notations et hypothèses

Pour tout N, l'exposant d'erreur K_N est indépendant du choix particulier de l'alphabet de quantification Ξ_N. Nous pouvons donc supposer sans perte de généralité que

$$\xi_{N,j} = \frac{\int_{C_{N,j}} y \, \mathrm{d}y}{\int_{C_{N,j}} \mathrm{d}y} \ ,$$

c'est-à-dire que chaque $\xi_{N,j}$ coïncide avec le centre de la cellule $C_{N,j}$. Définissons le volume et le diamètre de la cellule j par $V_{N,j} = \int_{C_{N,j}} \mathrm{d}y$ et $d_{N,j} = \sup_{u,v\in C_{N,j}} \|u - v\|$, respectivement. Nous introduisons alors la *densité spécifique* ζ_N et le *profil spécifique* M_N, fonctions constantes par morceaux sur Y respectivement définies de la manière suivante, pour tout $y \in C_{N,j}$ ($j \in \{1,\dots,N\}$) :

$$\begin{aligned} \zeta_N(y) = \ \zeta_{N,j} \ &= \frac{1}{NV_{N,j}} \ , \\ M_N(y) = M_{N,j} &= \frac{1}{V_{N,j}^{1+2/d}} \int_{C_{N,j}} (s - \xi_{N,j})(s - \xi_{N,j})^{\mathrm{T}} \, \mathrm{d}s \ . \end{aligned}$$

Nous considérons à présent une famille de quantificateurs $(\mathcal{C}_N, \Xi_N, \xi_N)_{N\geq 1}$, et faisons l'hypothèse suivante.

Hypothèse 4.3 (Quantification haute-résolution)**.**

1. Quand N tend vers l'infini, ζ_N converge uniformément vers une fonction continue ζ telle que $\inf_{y\in\mathsf{Y}} \zeta(y) > 0$.
2. Quand N tend vers l'infini, M_N converge uniformément vers une fonction continue (à valeurs matricielles) M telle que $\sup_{y\in\mathsf{Y}} \|M(y)\| < \infty$.
3. Il existe une constante C_d telle que, pour tout N, $\sup_j d_{N,j} \leq \dfrac{C_d}{N^{1/d}}$.

Nous appellerons ζ la *densité limite* de la famille $(\mathcal{C}_N, \Xi_N, \xi_N)_{N\geq 1}$. Elle représente la proportion de cellules dans le voisinage du point y. La fonction M sera appelée le *profil limite*. Pour tout $y \in \mathsf{Y}$, $M(y)$ est une matrice carrée non-négative de taille d. Elle donne des informations à propos de la forme des cellules. Dans la littérature, la fonction $y \mapsto \mathrm{Tr}\,(M(y))$ est appelée *profil d'inertie* [54, 61, 111].

Intuitivement, les quantificateurs haute-résolution doivent être construits de sorte que $\zeta(y)$ soit grande aux points y essentiels pour différencier les deux hypothèses. Le théorème 4.4 ci-dessous donne une formulation rigoureuse de cette intuition.

4.4.2 Exposant d'erreur dans le régime des hautes résolutions

Le résultat principal repose sur les hypothèses données ci-après. Pour tout $m \geq 0$ et tout $i \in \{0, 1\}$, définissons tout d'abord les quantités suivantes :

$$\eta_i(m) = \sup_{m'\geq m} \mathbb{E}_0 \left|\log p_i(Y_0|Y_{-m:-1}) - \log p_i(Y_0|Y_{-m':-1})\right| \ , \tag{4.5}$$
$$\eta_{i,N}(m) = \sup_{m'\geq m} \mathbb{E}_0 \left|\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1}) - \log p_{i,N}(Z_{N,0}|Z_{N,-m':-1})\right|$$

Notons que le théorème 4.2 et le corollaire 4.3 sont valables si les suites $\log p_i(Y_0|Y_{-m:-1})$ et $\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1})$ convergent dans $L^1(\mathbb{P}_0)$ quand $m \to \infty$, c'est-à-dire si $\eta_i(m)$ et $\eta_{i,N}(m)$ tendent vers zéro. Les coefficients $\eta_i(m)$ et $\eta_{i,N}(m)$ caractérisent plus précisément la vitesse de convergence de ces suites. L'hypothèse 4.4.3 ci-dessous assure que leurs limites sont atteintes suffisamment vite.

Hypothèse 4.4 (Douceur et oubli)**.**

1. Pour tout $n \geq 1$, $y_{1:n} \mapsto p_i(y_{1:n})$ est de classe C_3 sur Y^n.
2. $\sup_{\{n\geq 1, y_{1:n}\in\mathsf{Y}^n,\ 1\leq k,\ell,r\leq n,\ 1\leq h,\bar{\imath},\bar{\jmath}\leq d\}} \left|\frac{\partial^3 \log p_i}{\partial y_k^{(h)}\, \partial y_\ell^{(\bar{\imath})}\, \partial y_r^{(\bar{\jmath})}}(y_{1:n})\right| < \infty$.
3. Il existe deux constantes C_e, $\epsilon > 0$ telles que pour tous $i \in \{0, 1\}$, $N \geq 2$ et $m \geq 0$,

$$\max\left\{\eta_i(m)\,;\eta_{i,N}(m)\right\} \leq \frac{C_e}{(1+m)^{6+\epsilon}} \ . \tag{4.6}$$

4. Pour tout $i \in \{0,1\}$, tous entiers m,m',k tels que $-m' \leq -m \leq 0 \leq k$:

$$\mathbb{E}_0 \left\| \nabla_{y_0} \log p_i(Y_{0:k}|Y_{-m:-1}) - \nabla_{y_0} \log p_i(Y_{0:k}|Y_{-m':-1}) \right\| \leq \varphi_m \,, \tag{4.7}$$

$$\mathbb{E}_0 \left\| \nabla_{y_0} \log p_i(Y_k|Y_{-m:k-1}) \right\| \leq \psi_k \,, \tag{4.8}$$

où $\sum_k \varphi_k$ et $\sum_k \psi_k$ sont des séries convergentes.

Nous pouvons à présent énoncer le résultat principal. Rappelons que $p_0(y)$ est la densité de Y_0 sous $\mathbb{P}_0$, et que K et K_N sont les exposants d'erreur associés au test NP réalisé sur les observations parfaites et quantifiées, respectivement, donnés par (4.3) et (4.4). Notons que l'hypothèse 4.4.3 implique que les deux suites $\eta_i(m)$ et $\eta_{i,N}(m)$ tendent vers zéro. Cela garantit que, sous l'hypothèse 4.1, le théorème 4.2 et le corollaire 4.3 s'appliquent ; autrement dit, les exposants d'erreur K et K_N existent.

Théorème 4.4. *Sous les hypothèses 4.1, 4.3, 4.4 :*
Quand N tend vers l'infini, $N^{2/d}(K - K_N)$ converge vers la constante D_e donnée par

$$D_e = \frac{1}{2} \int \frac{p_0(y) F(y)}{\zeta(y)^{2/d}} \, \mathrm{d}y \,, \tag{4.9}$$

où la fonction F est définie par

$$F(y) = \mathbb{E}_0 \left[\ell(Y_{\mathbb{Z}})^{\mathrm{T}} M(Y_0) \, \ell(Y_{\mathbb{Z}}) \,\middle|\, Y_0 = y \right], \tag{4.10}$$

et la variable aléatoire $\ell(Y_{\mathbb{Z}})$ est la limite dans $L^2(\mathbb{P}_0)$ de la suite $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \right)_{k \geq 0}$.

Démonstration. Voir la section 4.5. □

Le théorème 4.4 indique que lorsque le nombre de points N du quantificateur tend vers l'infini, l'exposant d'erreur K_N converge à la vitesse $N^{-2/d}$ vers l'exposant d'erreur K correspondant au test NP réalisé directement sur les données non-quantifiées. La probabilité de manque $\beta_{N,n}(\alpha)$ du test NP de niveau α s'écrit donc approximativement de la manière suivante :

$$\beta_{N,n}(\alpha) \simeq e^{-n\left(K - \frac{D_e}{N^{2/d}}\right)} \tag{4.11}$$

lorsque le nombre n d'observations et le nombre N de points de quantification sont grands. La quantité D_e représente la perte (normalisée) en termes d'exposant d'erreur introduite par la quantification, dans le régime des hautes résolutions.

Notons que (4.9) ressemble à la formule de Bennett [8, Eq. (1.6)] et à son extension vectorielle [111, Eq. (7)].

Remarque 4.5. Le théorème 4.4 indique en particulier que, sous certaines conditions sur le processus observé, les quantificateurs *classiques*, tels ceux produits dans la perspective de minimiser l'EQM, conduisent à des exposants d'erreur K_N qui convergent vers K quand N tend vers l'infini, à la vitesse $N^{-2/d}$.

Remarque 4.6. Si les observations $(Y_k)_{k\geq 0}$ sont i.i.d. sous chacune des hypothèses, alors

$$F(y) = \nabla\Lambda(y)^{\mathrm{T}}\, M(y)\, \nabla\Lambda(y)\ ,$$

où $\Lambda(y) = \log \frac{p_0(y)}{p_1(y)}$ est le LRV d'un seul échantillon. Notons que l'expression (4.9) de D_e est cohérente avec celle de Gupta et Hero [61, Eq. (20)].

La perte asymptotique D_e dépend du quantificateur via sa densité limite ζ et son profil limite M. Dans les paragraphes suivants, nous étudions les valeurs de ces paramètres qui permettent de réduire cette perte.

4.4.3 Quantificateurs haute-résolution adaptés : Cas scalaire ($d = 1$)

Nous étudions tout d'abord le cas d'observations scalaires. Supposons alors que chaque cellule est connectée (les celules sont donc des intervalles), c'est-à-dire que le quantificateur est régulier [50]. Dans ce cas, $M_N(y) = 1/12$ pour tous y, N, et la fonction F s'écrit simplement

$$\begin{aligned} F(y) &= \frac{1}{12}\,\mathbb{E}_0\left[\ell(Y_{\mathbb{Z}})^2 \,\middle|\, Y_0 = y\right] \\ &= \frac{1}{12}\lim_{k\to\infty} \mathbb{E}_0\left[\left(\frac{\partial}{\partial y_0}\log\frac{p_0}{p_1}(Y_{-k:k})\right)^2 \,\middle|\, Y_0 = y\right]. \end{aligned}$$

En utilisant l'inégalité de Hölder dans (4.9), on montre alors aisément le résultat suivant.

Corollaire 4.5. *Si $d = 1$ et si les cellules sont des intervalles, alors la perte en exposant d'erreur D_e est telle que*

$$D_e \geq \frac{1}{2}\left(\int [p_0(y)F(y)]^{1/3}\,\mathrm{d}y\right)^3 . \tag{4.12}$$

Il y a égalité dans (4.12) si

$$\zeta(y) = \frac{[p_0(y)F(y)]^{1/3}}{\int [p_0(s)F(s)]^{1/3}\,\mathrm{d}s}\ .$$

La corollaire ci-dessus donne la règle de quantification haute-résolution optimale pour le test d'hypothèse initial.

Remarque 4.9. En pratique, un quantificateur scalaire à N points de densité limite ζ peut être facilement réalisé via un *compander*. Rappelons qu'un *compander* est la composition d'une fonction continue inversible ϕ (appelée compresseur) et d'un quantificateur uniforme [8, 54]. Il suffit alors de définir le compresseur ϕ comme la primitive de ζ sur Y. Par exemple, si Y est le segment $[a\,;b] \subset \mathbb{R}$, $\phi(x) = \int_a^x \zeta(t)\,\mathrm{d}t$, et la sortie du compresseur est uniformément quantifiée sur $[0\,;1]$. Si ζ est une fonction lipschitzienne, la suite de quantificateurs ainsi formée vérifie l'hypothèse 4.3, et sa densité limite est bien égale à ζ.

4.4.4 Quantificateurs haute-résolution adaptés : Cas vectoriel ($d \geq 2$)

Dans le cas vectoriel, la détermination des règles de quantification haute-résolution optimales nécessite la minimisation de l'expression (4.9) par rapport aux deux fonctions ζ et M. Malheureusement, comme indiqué dans [54, 116], on ne connaît pas les fonctions M acceptables comme profiles limites. La détermination de l'ensemble des paires (ζ, M) possibles est un problème ouvert, en dehors du périmètre de cette thèse.

Cependant, pour un profil M fixé, la densité ζ qui minimise D_e peut être facilement obtenue à partir de l'inégalité de Hölder :

$$D_e \geq \frac{1}{2} \left(\int [p_0(y) F(y)]^{\frac{d}{d+2}} \, \mathrm{d}y \right)^{\frac{d+2}{d}} ,$$

et il y a égalité si

$$\zeta(y) = \frac{[p_0(y) F(y)]^{\frac{d}{d+2}}}{\int [p_0(s) F(s)]^{\frac{d}{d+2}} \, \mathrm{d}s} . \tag{4.13}$$

En d'autres termes, on peut facilement calculer la stratégie de quantification haute-résolution optimale pour un profil limite donné. En suivant l'approche de [61], nous étudions deux types de profil limite.

4.4.4.1 Cellules congruentes à moment d'inertie minimal

Dans ce paragraphe, nous nous concentrons sur les quantificateurs dont les cellules sont congruentes à moment d'inertie minimal. Dans ce cas,

$$\forall\, y \in \mathsf{Y},\ M(y) = \nu I_d \, , \tag{4.14}$$

pour une certaine constante $\nu > 0$, et où I_d est la matrice identité de taille $d \times d$.

Rappelons que Gersho [49] fit la conjecture que, lorsque N tend vers l'infini, la plupart des cellules (toutes, sauf celles proches de la frontière du domaine considéré) d'un quantificateur à EQM minimale deviennent congruentes à un certain polytope H_d^*. Dans ce cas, $M(y)$ est indépendant de y. De plus, Zamir et Feder [173, Lemma 1] ont démontré que les cellules d'un quantificateur à EQM minimale deviennent des boules (donc à moment d'inertie minimal) lorsque la dimension d tend vers l'infini.

Pour les quantificateurs dont le profil limite est donné par (4.14), la densité limite optimale (4.13) devient

$$\zeta(y) = \frac{\left[p_0(y) \bar{F}(y)\right]^{\frac{d}{d+2}}}{\int \left[p_0(s) \bar{F}(s)\right]^{\frac{d}{d+2}} \, \mathrm{d}s} , \tag{4.15}$$

où la fonction $\bar{F}$ est définie par

$$\begin{aligned} \bar{F}(y) &= \mathbb{E}_0 \left[\|\ell(Y_{\mathbb{Z}})\|^2 \,\middle|\, Y_0 = y \right] \\ &= \lim_{k \to \infty} \mathbb{E}_0 \left[\left\| \nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \right\|^2 \,\middle|\, Y_0 = y \right] . \end{aligned} \tag{4.16}$$

Algorithme. En pratique, on souhaite concevoir un quantificateur dont la densité est proche de (4.15) pour un certain N fini. L'algorithme de Linde-Buzo-Gray (LBG) [93] peut être utilisé ici. Cet algorithme est une méthode itérative permettant de construire un quantificateur à N points à EQM minimale, à partir d'un ensemble d'apprentissage issu d'une certaine densité $p_0(y)$.

Un quantificateur à EQM minimale pour la densité p_0 minimise la quantité $\mathbb{E}_0\left[\left\|Y_0 - \xi_N(Y_0)\right\|^2\right]$. Un tel quantificateur possède la densité limite suivante [54, 111] :

$$\zeta_{EQM}(y) = \frac{p_0(y)^{\frac{d}{d+2}}}{\int p_0(s)^{\frac{d}{d+2}}\,\mathrm{d}s}\,. \tag{4.17}$$

En comparant (4.15) et (4.17), on remarque que le quantificateur proposé (de densité limite ζ donnée par (4.15)) peut être obtenu en pratique en exécutant l'algorithme LBG sur un ensemble d'apprentissage issu de la densité suivante :

$$q^*(y) = \frac{p_0(y)\bar{F}(y)}{\int p_0(s)\bar{F}(s)\,\mathrm{d}s}\,.$$

La section 4.7 donnent quelques illustrations de cette approche.

4.4.4.2 Cellules ellipsoïdales

De manière à obtenir quelque intuition sur la forme générale des cellules, et en suivant [61], nous étudions dans ce paragraphe les quantificateurs à cellules ellipsoïdales. De telles cellules ne peuvent bien sûr pas partitionner le domaine Y mais, pour de grandes dimensions d, par analogie avec l'approximation sphérique [29, 54, 173], nous pouvons supposer que la majorité des cellules d'un quantificateur donné sont d'une forme proche d'une ellipsoïde.

On peut alors montrer que les axes d'une cellule ellipsoïdale autour d'un point y doivent être alignés, dans l'ordre inverse, avec ceux de la matrice $\bar{L}(y)$ définie par

$$\bar{L}(y) = \mathbb{E}_0\left[\ell(Y_{\mathbb{Z}})\,\ell(Y_{\mathbb{Z}})^{\mathrm{T}}\,\middle|\,Y_0 = y\right]\,.$$

En particulier, son petit axe doit être aligné avec le vecteur propre principal de $\bar{L}(y)$ (voir la section 4.4.4.2 dans la partie II).

4.5 Démonstration du théorème 4.4

4.5.1 Préliminaires

Rappelons que $V_{N,j} = \int_{C_{N,j}} \mathrm{d}y$ est le volume de la cellule $C_{N,j}$ ($j \in \{1,\ldots,N\}$). Pour tout $i \in \{0,1\}$ et tout ensemble de points de quantification $\xi_{N,j_{1:n}} = (\xi_{N,j_1},\ldots,\xi_{N,j_n}) \in \Xi_N^n$,

on définit la densité normalisée de $Z_{N,1:n}$ par

$$\begin{aligned}\bar{p}_{i,N}(\xi_{N,j_{1:n}}) &= \frac{1}{V_{N,j_1} \times \cdots \times V_{N,j_n}}\, p_{i,N}(\xi_{N,j_{1:n}}) \\ &= \frac{1}{V_{N,j_1} \times \cdots \times V_{N,j_n}}\, P_{i,n}(C_{N,j_1} \times \cdots \times C_{N,j_n})\,. \end{aligned} \tag{4.18}$$

L'intérêt de cette définition réside dans le fait que $\bar{p}_{i,N}(\xi_{N,j_{1:n}}) \simeq p_i(\xi_{N,j_{1:n}})$ lorsque N est grand. Cette approximation sera de grande importance dans la suite. La fonction $\bar{p}_{i,N}(\xi_{N,j_n}|\xi_{N,j_{1:n-1}})$ est définie de manière similaire.

Pour tout $i \in \{0,1\}$ et tout entier $\ell \geq 0$, on introduit les fonctions suivantes :

$$\begin{aligned}&\forall\, y_{-\ell:0} \in \mathsf{Y}^{\ell+1}, \qquad \mathcal{L}_i(y_{-\ell:0}) = \log p_i(y_0|y_{-\ell:-1})\,, \\ &\forall\, z_{-\ell:0} \in \Xi_N^{\ell+1}, \quad \mathcal{L}_{i,N}(z_{-\ell:0}) = \log \bar{p}_{i,N}(z_0|z_{-\ell:-1})\,.\end{aligned}$$

En raison des hypothèses 4.1.3 et 4.4.3, la suite aléatoire $(\mathcal{L}_i(Y_{-\ell:0}))_{\ell\geq 0}$ appartient à $L^1(\mathbb{P}_0)$. De plus, l'hypothèse 4.4.3 pour m grand assure que la suite $(\mathcal{L}_i(Y_{-\ell:0}))_{\ell\geq 0}$ est une suite de Cauchy de $L^1(\mathbb{P}_0)$. Notons $\mathcal{L}_i(Y_{-\infty:0})$ sa limite. D'après l'hypothèse 4.4.3, l'inégalité suivante est valable pour tout $\ell \geq 0$:

$$\mathbb{E}_0|\mathcal{L}_i(Y_{-\ell:0}) - \mathcal{L}_i(Y_{-\infty:0})| \leq \frac{C_e}{(1+\ell)^{\,6+\epsilon}}\,. \tag{4.19}$$

Un résultat similaire existe pour la suite $(\mathcal{L}_{i,N}(Z_{N,-\ell:0}))_{\ell\geq 0}$, qui converge dans $L^1(\mathbb{P}_0)$ vers une variable aléatoire $\mathcal{L}_{i,N}(Z_{N,-\infty:0})$ et vérifie l'inégalité suivante, pour tout $\ell \geq 0$:

$$\mathbb{E}_0|\mathcal{L}_{i,N}(Z_{N,-\ell:0}) - \mathcal{L}_{i,N}(Z_{N,-\infty:0})| \leq \frac{C_e}{(1+\ell)^{\,6+\epsilon}}\,. \tag{4.20}$$

Notre but est d'étudier la différence $K - K_N$ entre les exposants d'erreur associés au test NP réalisé avec et sans quantification. Cette différence s'écrit

$$K - K_N = (K_0 - K_{0,N}) - (K_1 - K_{1,N})\,, \tag{4.21}$$

où, pour tout $i \in \{0,1\}$,

$$\begin{aligned}K_i &= \mathbb{E}_0\left[\mathcal{L}_i(Y_{-\infty:0})\right]\,, \\ K_{i,N} &= \mathbb{E}_0\left[\mathcal{L}_{i,N}(Z_{N,-\infty:0})\right]\,.\end{aligned}$$

Dans la suite, nous nous concentrons sur l'étude de $K_1 - K_{1,N}$, celle de $K_0 - K_{0,N}$ étant similaire.

Prenons ϵ' tel que $0 < \epsilon' < \frac{\epsilon}{3d(6+\epsilon)}$, et définissons la suite d'entiers $m = m(N) = \lfloor N^{1/(3d)-\epsilon'} \rfloor$. Notons alors que

$$\lim_{N\to\infty} \frac{m^3}{N^{1/d}} = 0\,. \tag{4.22}$$

La décomposition suivante est fondamentale : $K_{1,N} = K_1 + T_N + U_N + \delta_N$, où

$$
\begin{aligned}
T_N &= \mathbb{E}_0\left[\mathcal{L}_{1,N}(Z_{N,-m:0}) - \mathcal{L}_1(Z_{N,-m:0})\right] \ , \\
U_N &= \mathbb{E}_0\left[\mathcal{L}_1(Z_{N,-m:0}) - \mathcal{L}_1(Y_{-m:0})\right] \ , \\
\delta_N &= \mathbb{E}_0\left[\mathcal{L}_{1,N}(Z_{N,-\infty:0}) - \mathcal{L}_{1,N}(Z_{N,-m:0})\right] + \mathbb{E}_0\left[\mathcal{L}_1(Y_{-m:0}) - \mathcal{L}_1(Y_{-\infty:0})\right] \ .
\end{aligned}
$$

D'après (4.19) et (4.20),

$$
N^{2/d}|\delta_N| \leq 2\, C_e\, \frac{N^{2/d}}{(1+m)^{\,6+\epsilon}} \ .
$$

Par définition de la suite $m = m(N)$, $N^{2/d}|\delta_N|$ tend vers zéro quand $N \to \infty$. Par conséquent, l'analyse asymptotique de la quantité $N^{2/d}(K_{1,N} - K_1)$ se résume à celle de T_N et U_N.

Comme Y est un ensemble borné, l'hypothèse 4.4.2 permet d'obtenir les bornes suivantes sur les dérivées de la densité p_1 :

$$
\sup_{\{y_{1:n} \in \mathsf{Y}^n,\, 1 \leq k \leq n\}} \|\nabla_{y_k} \log p_1(y_{1:n})\| \leq C_1 \ , \tag{4.23}
$$

$$
\sup_{\{y_{1:n} \in \mathsf{Y}^n,\, 1 \leq k \leq n\}} \left\|\nabla^2_{y_k} \log p_1(y_{1:n})\right\| \leq C_2 \ , \tag{4.24}
$$

où C_1 et C_2 sont des constantes.

4.5.2 Étude de T_N

T_N se décompose de la manière suivante :

$$
T_N = \mathbb{E}_0\left[\log \frac{\bar{p}_{1,N}(Z_{N,-m:0})}{p_1(Z_{N,-m:0})}\right] - \mathbb{E}_0\left[\log \frac{\bar{p}_{1,N}(Z_{N,-m:-1})}{p_1(Z_{N,-m:-1})}\right] \ . \tag{4.25}
$$

Nous étudions chaque terme du membre de droite de cette équation. Considérons $u \in \{-1, 0\}$. Le lemme suivant est une conséquence du développement de Taylor de la fonction $y_{-m:u} \mapsto p_1(y_{-m:u})$ au point $\xi_{N,j_{-m:u}}$, en utilisant les hypothèses 4.3.3, 4.4, et les propriétés de la suite de quantificateurs.

Lemme 4.6. *Pour tout $j_{-m:u} \in \{1, \ldots, N\}^{u+m+1}$,*

$$
\frac{\bar{p}_{1,N}(\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} = 1 + \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} Tr\left(\frac{\nabla^2_{y_k} p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}}}{p_1(\xi_{N,j_{-m:u}})} \frac{M_{N,j_k}}{\zeta^{2/d}_{N,j_k}}\right) + \epsilon_{N,j_{-m:u}} \ ,
$$

où $\left|\epsilon_{N,j_{-m:u}}\right| \leq c_T \left(\frac{m+1}{N^{1/d}}\right)^3$, et c_T est une constante.

Démonstration. Voir l'annexe F.1. □

En injectant l'équation ci-dessus dans (4.25), en utilisant l'inégalité $\big|\log(1+x)-x\big| \leq x^2$ (au voisinage de zéro), les hypothèses 4.3, 4.4.2, et (4.22), on obtient

$$T_N = T_N(0) - T_N(-1) + o_N(N^{-2/d}) \,, \tag{4.26}$$

où, pour tout $u \in \{-1, 0\}$,

$$T_N(u) = \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\mathrm{Tr} \left(\frac{\nabla^2_{y_k} p_1(Z_{N,-m:u})^{\mathrm{T}}}{p_1(Z_{N,-m:u})} \, \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \right) \right] . \tag{4.27}$$

4.5.3 Étude de U_N

U_N se décompose de la manière suivante :

$$U_N = \mathbb{E}_0\big[\log p_1(Z_{N,-m:0}) - \log p_1(Y_{-m:0})\big] - \mathbb{E}_0\big[\log p_1(Z_{N,-m:-1}) - \log p_1(Y_{-m:-1})\big] \,. \tag{4.28}$$

Étudions chaque terme du membre de droite de cette égalité. Pour tous $u \in \{-1, 0\}$, $j_{-m:u} \in \{1, \dots, N\}^{u+m+1}$, développons $y_{-m:u} \mapsto \log p_1(y_{-m:u})$ au point $\xi_{N,j_{-m:u}}$:

$$\begin{aligned} \log p_1(y_{-m:u}) = \log p_1(\xi_{N,j_{-m:u}}) + \sum_{k=-m}^{u} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} \, (y_k - \xi_{N,j_k}) \\ + \frac{1}{2} \sum_{k,\ell=-m}^{u} (y_k - \xi_{N,j_k})^{\mathrm{T}} \, \nabla^2_{y_k,y_\ell} \log p_1(\xi_{N,j_{-m:u}}) \, (y_\ell - \xi_{N,j_\ell}) + \epsilon'_N(y_{-m:u}) \,. \end{aligned} \tag{4.29}$$

Sous les hypothèses 4.33 et 4.4.2, pour tout $y_{-m:u} \in C_{N,j_{-m}} \times \cdots \times C_{N,j_u}$, le reste vérifie l'inégalité suivante :

$$\big|\epsilon'_N(y_{-m:u})\big| \leq (m+1)^3 \, c'_3 \left(\frac{C_d}{N^{1/d}} \right)^3 \,,$$

où c'_3 est une constante. D'après (4.22), le membre de droite de cette inégalité tend vers zéro quand N tend vers l'infini, plus vite que $N^{-2/d}$. En injectant le développement de Taylor (4.29) dans l'expression (4.28) de U_N, on obtient

$$U_N = U_N(0) - U_N(-1) + o_N(N^{-2/d}) \,, \tag{4.30}$$

où, pour tout $u \in \{-1, 0\}$,

$$\begin{aligned} U_N(u) = - \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \, (Y_k - Z_{N,k}) \right] \\ - \frac{1}{2} \sum_{k,\ell=-m}^{u} \mathbb{E}_0 \left[(Y_k - Z_{N,k})^{\mathrm{T}} \, \nabla^2_{y_k,y_\ell} \log p_1(Z_{N,-m:u}) \, (Y_\ell - Z_{N,\ell}) \right] \,. \end{aligned} \tag{4.31}$$

L'étape suivante consiste à étudier les termes dominants du membre de droite de (4.31).

Lemme 4.7. *Pour tout $u \in \{-1, 0\}$,*

$$U_N(u) = A_N(u) + B_N(u) + o_N(N^{-2/d}) \,,$$

où A_N et B_N sont définis de la manière suivante :

$$A_N(u) = -\frac{1}{N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:u}) \right] , \quad (4.32)$$

$$B_N(u) = -\frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[Tr \left(\nabla^2_{y_k} \log p_1(Z_{N,-m:u}) \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \right) \right] .$$

Démonstration. Voir l'annexe F.2. □

Nous décomposons à présent le terme $\nabla^2_{y_k} \log p_1$:

$$\nabla^2_{y_k} \log p_1(y_{-m:u}) = \frac{\nabla^2_{y_k} p_1(y_{-m:u})}{p_1(y_{-m:u})} - \frac{\nabla_{y_k} p_1(y_{-m:u}) \nabla_{y_k} p_1(y_{-m:u})^{\mathrm{T}}}{(p_1(y_{-m:u}))^2} .$$

D'après cette décomposition et (4.27), nous pouvons diviser $B_N(u)$ en deux termes :

$$B_N(u) = -T_N(u) + \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\mathrm{Tr} \left(\nabla_{y_k} \log p_1(Z_{N,-m:u}) \nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \right) \right] . \quad (4.33)$$

En développant la fonction $\nabla_{y_k} \log p_1$ dans l'équation ci-dessus et dans (4.32), on peut écrire le terme dominant plus simplement, en remplaçant chaque Z_N par Y. Sous l'hypothèse 4.3, d'après (4.24) et (4.22), les restes correspondants sont des $o_N(N^{-2/d})$. Au final :

$$\begin{aligned} U_N(u) = &-\frac{1}{N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:u}) \right] \\ &+ \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_1(Y_{-m:u}) \right] \\ &- T_N(u) + o_N(N^{-2/d}) . \end{aligned} \quad (4.34)$$

4.5.4 Fin de la démonstration

Les lemmes suivants se démontrent à partir des résultats des sections 4.5.2 et 4.5.3.

Lemme 4.8.

$$N^{2/d}(K - K_N) = \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-m:0}) \right] + \sum_{k=-m}^{-1} \mathbb{E}_0 \left[\mathcal{H}_{N,k}(Y_{-m:0}) - \mathcal{H}_{N,k}(Y_{-m:-1}) \right] + o_N(1) , \quad (4.35)$$

où, pour tout $u \in \{-1, 0\}$, *tout* $m \geq 1$ *et tout* $k \in \{-m, \ldots, u\}$:

$$\mathcal{H}_{N,k}(Y_{-m:u}) = \frac{1}{2} \nabla_{y_k} \log \frac{p_0}{p_1}(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log \frac{p_0}{p_1}(Y_{-m:u}) . \quad (4.36)$$

Démonstration. Voir la section 4.5.4 dans la partie II. □

Étudions à présent la série (4.35). Sous les hypothèses 4.3, 4.4.2 et 4.4.4, les propriétés d'oubli suivantes sont valables pour tous entiers positifs ℓ', ℓ et tous entiers k, u tels que $-\ell' \leq -\ell \leq k \leq u$:

$$\mathbb{E}_0 \left| \mathcal{H}_{N,k}(Y_{-\ell:u}) - \mathcal{H}_{N,k}(Y_{-\ell':u}) \right| \leq c_h \varphi_{\ell-|k|} \,, \tag{4.37}$$

$$\mathbb{E}_0 \left| \mathcal{H}_{N,k}(Y_{-\ell:0}) - \mathcal{H}_{N,k}(Y_{-\ell:-1}) \right| \leq c_h \psi_{|k|} \,, \tag{4.38}$$

où c_h est une constante.

Il est clair d'après (4.37) que la suite $(\mathcal{H}_{N,k}(Y_{-\ell:u})))_{\ell \geq -u}$ est une suite de Cauchy dans $L^1(\mathbb{P}_0)$. Notons $\mathcal{H}_{N,k}(Y_{-\infty:u})$ sa limite. Les inégalités (4.37) et (4.38) constituent les principaux outils pour l'analyse asymptotique de la série (4.35).

Lemme 4.9.

$$N^{2/d}(K - K_N) = \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-\infty:0}) \right] + \sum_{k=-\infty}^{-1} \mathbb{E}_0 \left[\mathcal{H}_{N,k}(Y_{-\infty:0}) - \mathcal{H}_{N,k}(Y_{-\infty:-1}) \right] + o_N(1) \,.$$

Démonstration. Voir l'annexe F.3. □

Comme le processus $(Y_k)_{k\in\mathbb{Z}}$ est stationnaire, l'espérance $\mathbb{E}_0$ dans la somme ci-dessus est invariante par changement d'origine des temps. Après quelques manipulations, on obtient

$$N^{2/d}(K - K_N) = \lim_{k\to\infty} \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-\infty:k}) \right] + o_N(1) \,. \tag{4.39}$$

Pour $k \geq 0$ fixé, (4.7) assure que la suite $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-m:k}) \right)_{m\geq 0}$ est une suite de Cauchy de $L^1(\mathbb{P}_0)$. Notons $\ell_k(Y_{-\infty:k})$ sa limite. La majoration (4.8) est uniforme en m ; par conséquent, elle est également valable pour la suite $(\ell_k(Y_{-\infty:k}))_{k\geq 0}$:

$$\mathbb{E}_0 \left\| \ell_k(Y_{-\infty:k}) - \ell_{k-1}(Y_{-\infty:k-1}) \right\| \leq \psi_k \,.$$

Sous l'hypothèse 4.4.4, $\sum_k \psi_k$ est une série convergente. La suite $(\ell_k(Y_{-\infty:k}))_{k\geq 0}$ est donc une suite de Cauchy de $L^1(\mathbb{P}_0)$. Notons $\ell(Y_{\mathbb{Z}})$ sa limite. La majoration (4.7) (resp. (4.8)) est uniforme en m' (resp. m) ; on peut alors facilement prouver que $\ell(Y_{\mathbb{Z}})$ coïncide avec la limite dans $L^1(\mathbb{P}_0)$ de la suite $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \right)_{k\geq 0}$.

D'après (4.23) et son équivalent pour la densité p_0, la quantité $\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k})$ est uniformément bornée. La limite ci-dessus est donc également une limite au sens $L^2(\mathbb{P}_0)$:

$$\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \xrightarrow[k\to\infty]{L^2(\mathbb{P}_0)} \ell(Y_{\mathbb{Z}}) \,. \tag{4.40}$$

En injectant (4.36) et (4.40) dans (4.39), et en faisant tendre N vers l'infini, on démontre le théorème 4.4. □

4.6 Illustration : Processus de Markov cachés

Dans cette section, nous traduisons les hypothèses de ce chapitre dans le cas de modèles de Markov cachés. Pour de tels modèles, elles se réduisent à des conditions simples sur le noyau de transition de la chaîne de Markov sous-jacente, et sur le noyau d'observation. Ce contexte, où les observations sont des échantillons bruités d'une certaine chaîne de Markov, a été récemment l'objet de nombreux travaux dans le domaine des réseaux de capteurs [62, 144].

Considérons un processus stationnaire markovien $(X_k)_{k\geq 0}$ à valeurs dans un espace d'état arbitraire X, et jouant le rôle d'une source à détecter. Pour tout $i \in \{0,1\}$ et tout entier t, on suppose que le noyau de transition (itéré) $\mathbb{P}_i\left[X_{k+t} \in \cdot \,|\, X_k = x\right]$ admet une densité $x' \mapsto q_i^t(x,x')$ par rapport à une mesure de probabilité λ sur $(\mathsf{X}, B(\mathsf{X}))$. On suppose également qu'il existe un entier m, et deux réels σ^-, σ^+ tels que, pour tout $i \in \{0,1\}$ et tout $(x,x') \in \mathsf{X}^2$, $0 < \sigma^- \leq q_i^m(x,x') \leq \sigma^+$. Cela implique en particulier que la chaîne de Markov $(X_k)_{k\in\mathbb{Z}}$ est de support borné.

Notons que, si l'espace d'état X est fini, ces conditions sont vérifiées si la chaîne $(X_k)_{k\in\mathbb{Z}}$ est *irréductible apériodique*, en définissant λ comme la mesure de comptage (normalisée) sur X. Dans ce cas, la chaîne admet une loi stationnaire, et $q_i^m(x,x') > 0$ pour tout x, x', et un certain entier m [16, Section 8].

Les états X_k de la chaîne de Markov sont supposés cachés. Seule une version « bruitée » Y_k ($\in \mathsf{Y} \subset \mathbb{R}^d$) de X_k est disponible au capteur k. Supposons que la distribution $\mathbb{P}[Y_k \in \cdot\,|X_k = x]$ ne dépend pas de l'hypothèse H0 ou H1, et qu'elle admet une densité $y \mapsto g(x,y)$ par rapport à la mesure de Lebesgue (restreinte à Y) μ, telle que $0 < \inf_{x,y} g(x,y) \leq \sup_{x,y} g(x,y) < \infty$. Nous supposons de plus que cette densité vérifie les hypothèses de douceur suivantes : pour tout $x \in \mathsf{X}$, $y \mapsto g(x,y)$ est de classe C_3 sur Y, et $\sup_{\{x\in\mathsf{X},\, y\in\mathsf{Y},\, 1\leq h,\bar{\imath},\bar{\jmath}\leq d\}} \left|\frac{\partial^3 g}{\partial y^{(h)}\,\partial y^{(\bar{\imath})}\,\partial y^{(\bar{\jmath})}}(x,y)\right| < \infty$. La situation est représentée à la figure 4.1.

De telles hypothèses ont été récemment proposées pour l'étude du comportement asymptotique de la log-vraisemblance $\log p_i(Y_{1:n})$ quand n tend vers l'infini [23, 37]. En particulier, il est montré que

$$\left|\log p_i(Y_0|Y_{-m:-1}) - \log p_i(Y_0|Y_{-m':-1})\right| \leq \frac{2}{1-\sigma^-/\sigma^+}\left(\frac{\sigma^-}{\sigma^+}\right)^{m-1},$$

pour tous $m' \geq m \geq 0$. Cela prouve que la suite $\log p_i(Y_0|Y_{-m:-1})$ converge dans $L^1(\mathbb{P}_0)$ quand $m \to \infty$, et donne l'hypothèse 4.2. De plus, cette convergence a lieu à une vitesse exponentielle ; les quantités $\eta_i(m)$, définies par (4.5), tendent donc vers zéro à une vitesse supérieure à $1/m^6$. Il en est de même pour les coefficients $\eta_{i,N}(m)$, sans hypothèse particulière sur le quantificateur : la quantification conserve le caractère « markovien caché » du processus original $(Y_k)_{k\in\mathbb{Z}}$. L'hypothèse 4.4.3 est donc vérifiée.

Les hypothèses 4.4.1 et 4.4.2 sont des conséquences directes des conditions de douceur de g données ci-dessus. L'hypothèse 4.4.4 peut être démontrée en suivant le raisonnement

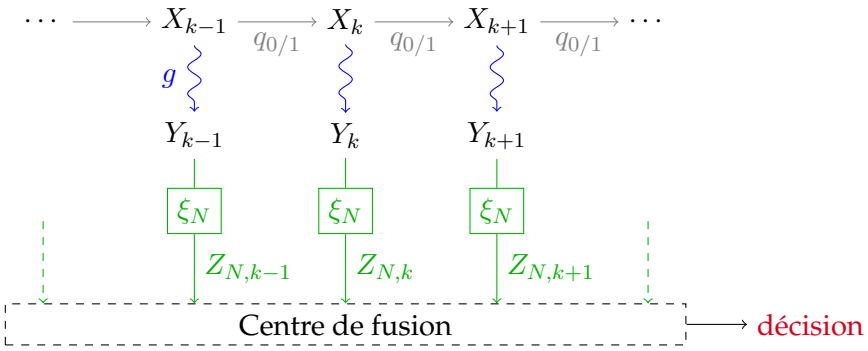


Figure 4.1 – Détection d'un processus markovien à partir d'une version bruitée.

de [23,37]. La proposition suivante est donc une conséquence des résultats de [23,37]. La démonstration est omise.

Proposition 4.10. *Les conditions données par les hypothèses 4.1 et 4.4 sont vérifiées par le processus $(Y_k)_{k\in\mathbb{Z}}$ décrit dans cette section.*

Par conséquent, si la famille de quantificateurs vérifie l'hypothèse 4.3, alors les théorèmes 4.2 et 4.4 s'appliquent.

La section 4.7.1 ci-après donne un exemple pratique d'un tel problème de détection.

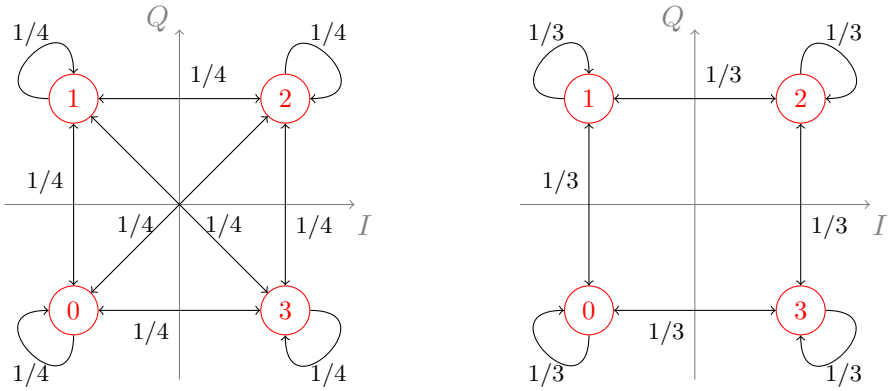
4.7 Résultats numériques

Dans cette section, nous illustrons nos résultats dans plusieurs contextes en comparant les quantificateurs suivants :

- le *quantificateur proposé*, obtenu en suivant l'approche décrite à la section 4.4.4.1 et dont la densité limite est donnée par (4.15) ;
- le *quantificateur à EQM minimale*, qui minimise $\mathbb{E}_0 \|Y_0 - Z_{N,0}\|^2$ et dont la densité limite est donnée par (4.17);
- le *quantificateur de Gupta-Hero* [61] : dans ce cas, la densité limite est calculée comme si les observations étaient i.i.d., en tenant compte des seules distributions marginales $p_0(y)$ et $p_1(y)$;
- le *quantificateur uniforme*, dont la densité limite est constante.

4.7.1 Détection de modulation : QPSK vs. OQPSK

Dans cette section, nous donnons un exemple de modèles de Markov cachés qui vérifient les hypothèses données à la section 4.6, et détaillons la conception de quantificateurs pratiques en suivant l'approche de la section 4.4.4.1.



(a) QPSK (b) OQPSK

Figure 4.2 – QPSK vs. OQPSK – Constellations et probabilités de transition.

4.7.1.1 Modèle d'observation

Considérons le modèle suivant pour des observations de dimension $d = 2$:

$$Y_k = T(X_k) + W_k \,, \tag{4.41}$$

où $(X_k)_{k\in\mathbb{Z}}$ est un message à valeurs dans $\mathsf{X} = \{0, 1, 2, 3\}$, $T(x)$ est la représentation de l'état x dans le plan en-phase/quadrature[1] (voir la figure 4.2), et $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, \sigma^2)$ est un bruit gaussien circulaire de moyenne nulle et de variance σ^2. Le processus $(X_k)_{k\in\mathbb{Z}}$ est i.i.d. et uniformément distribué sous H0, et forme une chaîne de Markov sous H1 :

$$\begin{aligned} &\mathsf{H0} : \; X_k \overset{\text{i.i.d.}}{\sim} \mathcal{U}_{\{0,1,2,3\}} \\ &\mathsf{H1} : \; X_0 \sim \mathcal{U}_{\{0,1,2,3\}}, \; \mathbb{P}_1[X_{k+1} = x' | X_k = x] = q(x, x') \,, \end{aligned}$$

où q est la matrice de transition de la chaîne de Markov, donnée par :

$$q = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \end{bmatrix} .$$

Cette situation correspond au test, à partir d'observations bruitées, entre deux modulations à quatre états, *quadrature phase-shift keying* (QPSK) et *offset quadrature phase-shift keying* (OQPSK), dans le plan en-phase/quadrature [133, Chapter 3]. Les constellations correspondantes sont représentées à la figure 4.2.

[1] $T(0) = \begin{bmatrix} -1 \\ -1 \end{bmatrix}, T(1) = \begin{bmatrix} -1 \\ 1 \end{bmatrix}, T(2) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, T(3) = \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$

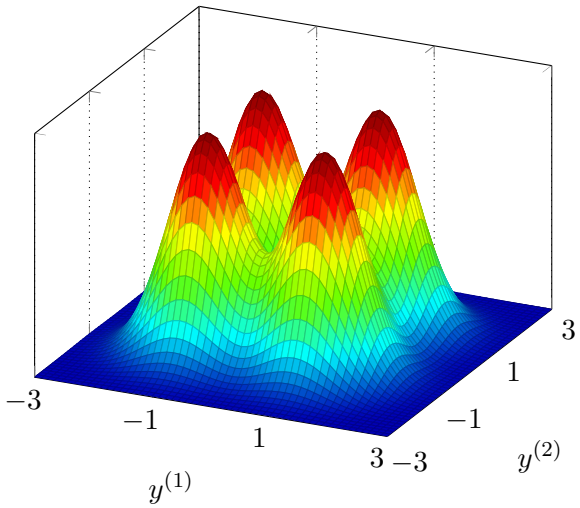


Figure 4.3 – QPSK vs. OQPSK – Densité marginale des observations $p_0(y) = p_1(y)$ ($M = 3$, $\sigma = 0.6$).

Dans le modèle d'observation (4.41), les densités ont un support infini. Nous considérons donc des observations tronquées sur $\mathsf{Y} = [-M\,;M]^2$, pour un réel positif M fixé [71, Section 10.1]. Le nouveau processus (tronqué) est un modèle de Markov caché de densité d'observation $g(x, y)$ donnée par

$$g(x,y) = \frac{\mathbf{1}_{[-M;M]^2}(y)}{C_M(\sigma)} \exp\left(\frac{-1}{2\sigma^2}(y - T(x))^{\mathrm{T}}(y - T(x))\right) , \tag{4.42}$$

où $\mathbf{1}_A$ représente l'indicatrice de l'ensemble A, et $C_M(\sigma)$ est une constante telle que $\int_{\mathsf{Y}} g(x, y)\,\mathrm{d}y = 1$ pour tout $x \in \{0, 1, 2, 3\}$.

Ce modèle de Markov caché vérifie les hypothèses données à la section 4.6. D'après la proposition 4.10, si la famille de quantificateurs vérifie l'hypothèse 4.3, alors les théorèmes 4.2 et 4.4 s'appliquent.

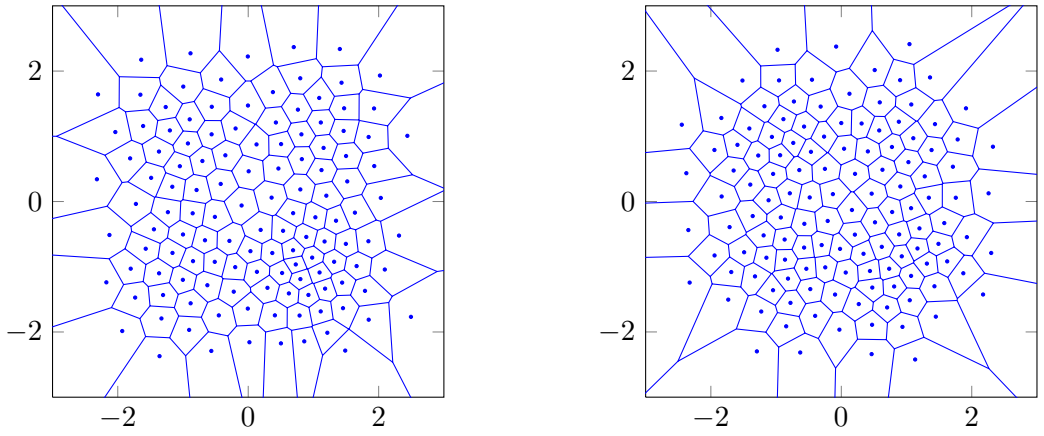
Notons que la densité marginale des observations $(Y_k)_{k\geq 0}$ (représentée à la figure 4.3) s'écrit

$$p_0(y) = p_1(y) = \frac{1}{4}\sum_{x=0}^{3} g(x, y) . \tag{4.43}$$

Comme celle-ci ne dépend pas de l'hypothèse, le quantificateur de Gupta-Hero [61], qui minimise la perte en exposant d'erreur dans le cas d'observations i.i.d., n'est pas défini.

4.7.1.2 Exemples de quantificateurs

La figure 4.4a représente un quantificateur à EQM minimale à 128 cellules construit par l'algorithme LBG, pour $M = 3$, $\sigma = 0.6$; la figure 4.4b, le quantificateur proposé correspondant. Ce dernier diffère de celui à EQM minimale : certains points de faible probabilité se révèlent significatifs pour le problème de détection considéré. Nous donnons ci-dessous quelques détails sur la méthode utilisée pour obtenir ces quantificateurs.



(a) Quantificateur à EQM minimale

(b) Quantificateur proposé

Figure 4.4 – QPSK vs. OQPSK – Quantificateurs à 128 cellules ($M = 3$, $\sigma = 0.6$, 20 000 échantillons).

Quantificateur à EQM minimale. Le quantificateur à EQM minimale de la figure 4.4a a été obtenu par l'algorithme LBG, à partir de 20 000 échantillons de distribution $\mathbb{P}_0$, c'est-à-dire i.i.d. de densité $p_0(y)$ (représentée à la figure 4.3).

Quantificateur proposé. Comme indiqué à la section 4.4.4.1, le quantificateur proposé, dont la densité limite ζ est donnée par (4.15), peut être construit en pratique via l'algorithme LBG à partir d'observations de densité

$$q^*(y) = \frac{p_0(y)\bar{F}(y)}{\int p_0(s)\bar{F}(s)\,\mathrm{d}s}\,.$$

Nous avons simulé 20 000 échantillons de cette densité par la méthode du rejet [94, Section 2.2]. En pratique, la fonction $\bar{F}$ donnée par (4.16) a été approchée par

$$\bar{F}_k(y) = \frac{1}{n_{MC}} \sum_{j=1}^{n_{MC}} \left\| \nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:-1}(j), y, Y_{1:k}(j)) \right\|^2 , \tag{4.44}$$

pour $k = 3$ et $n_{MC} = 1\ 000$, soit au total 6 000 échantillons i.i.d. de densité p_0. Ces valeurs ont été choisies sur la base d'observations empiriques.

Le gradient dans (4.44) s'écrit de la manière suivante (après quelques manipulations et en utilisant (4.42), (4.43)) :

$$\begin{aligned}\nabla_{y_0} \log \frac{p_0}{p_1}(y_{-k:k}) &= \nabla_{y_0} \log p_0(y_0) - \nabla_{y_0} \log p_1(y_{-k:k}) \\ &= \frac{1}{\sigma^2} \left\{ \frac{\mathbb{E}_0\left[T(X_0)\, g(X_0, y_0)\right]}{\mathbb{E}_0\left[g(X_0, y_0)\right]} - \frac{\mathbb{E}_1\left[T(X_0) \prod_{j=-k}^{k} g(X_j, y_j)\right]}{\mathbb{E}_1\left[\prod_{j=-k}^{k} g(X_j, y_j)\right]} \right\} .\end{aligned}$$

Comme ce sont des sommes finies sur X et X^{2k+1}, les quatre espérances ci-dessus peuvent être calculées de manière exacte lors de l'évaluation de $\bar{F}_k$ (4.44).

4.7.2 Détection d'une structure AR dans un signal gaussien 2-D

Considérons le modèle suivant pour des observations de dimension $d = 2$:

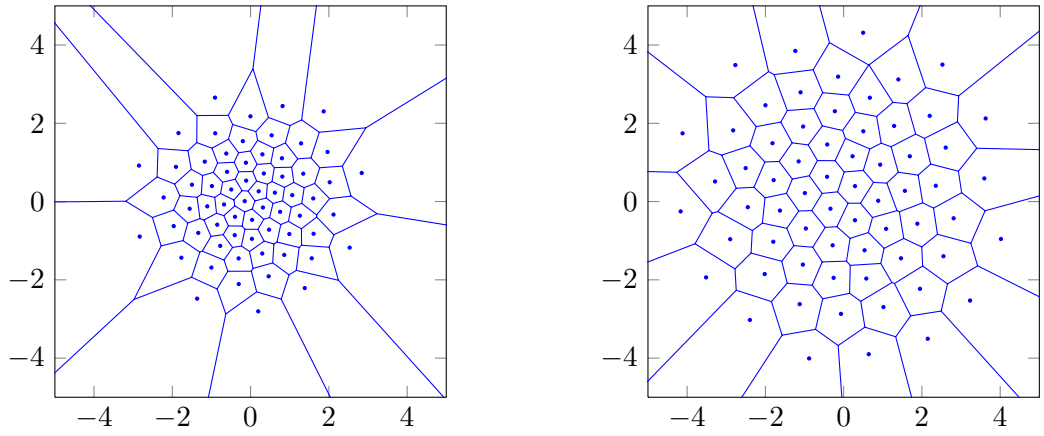
$$Y_k = X_k + W_k \ ,$$

où $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, \sigma^2)$ est un bruit gaussien circulaire de moyenne nulle et de variance σ^2, et $(X_k)_{k\in\mathbb{Z}}$ est un processus gaussien, blanc sous $\mathsf{H}0$ et corrélé (AR-1) sous $\mathsf{H}1$. Plus précisément,

$$\begin{aligned} \mathsf{H}0 &: \ X_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0,1) \\ \mathsf{H}1 &: \ X_k = aX_{k-1} + \sqrt{1-a^2}\, U_k \ , \end{aligned}$$

où $a \in \,]0\,;1[$ est le coefficient de corrélation et $U_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0,1)$ le processus d'innovation. En particulier, $(Y_k)_{k\in\mathbb{Z}}$ est un processus blanc gaussien sous $\mathsf{H}0$, et un processus de Markov caché sous $\mathsf{H}1$. La loi marginale d'une seule observation est identique sous les deux hypothèses.

Notons que, dans ce modèle, les densités ont un support infini ; les hypothèses de ce chapitre ne sont pas satisfaites (l'espace d'observation Y est égal à $\mathbb{R}^2$, il est donc non borné). En particulier, le théorème 4.4 ne s'applique pas. Cependant, dans le but d'obtenir quelque intuition sur la conception pratique de quantificateurs pour la détection, nous pouvons toujours utiliser l'approche décrite à la section 4.4.4.1 et calculer la densité limite proposée (4.15).



(a) Quantificateur à EQM minimale

(b) Quantificateur proposé

Figure 4.5 – Détection d'une structure AR – Quantificateurs à 64 cellules ($a = 0.8$, $\sigma = 1$, 20 000 échantillons).

La figure 4.5a représente un quantificateur à EQM minimale à 64 cellulles construit par l'algorithme LBG (à partir de $20\,000$ échantillons d'apprentissage), pour $\sigma = 1$; la figure 4.5b le quantificateur proposé correspondant, pour $a = 0.8$. Ce dernier diffère de manière significative du précédent. Les points de faible probabilité semblent significatifs pour ce problème de détection.

4.7.3 Détection d'un processus MA dans du bruit

Soient $(Y_k)_{k\in\mathbb{Z}}$ les échantillons collectés par un récepteur qui souhaite décider entre les deux hypothèses suivantes :

$$\begin{aligned} \mathsf{H0} &: \; Y_k = W_k \;, \\ \mathsf{H1} &: \; Y_k = \sum_{\ell=0}^{L} h_\ell \, U_{k-\ell} + W_k \;. \end{aligned}$$

où $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0, \sigma^2)$ est un bruit blanc gaussien (scalaire), et U_k est une source aléatoire observée via un canal de propagation de coefficients (réels, déterministes) $h_0, \ldots, h_L$ (L est un entier qui représente la mémoire du canal). Dans la suite, nous supposons que $L = 3$ et que la source est gaussienne : $U_k \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0, 1)$. Nous étudions le cas où le capteur réalise une quantification (scalaire) du signal reçu avant transmission au centre de décision.

De même que dans la section 4.7.2, les densités dans ce modèle ont un support infini ; l'approche décrite à la section 4.4.4.1 peut tout de même être utilisée pour la conception pratique de quantificateurs adaptés.

Pour les même raisons, le résultat de Gupta et Hero [61, Eq. (20)] n'est pas valable,

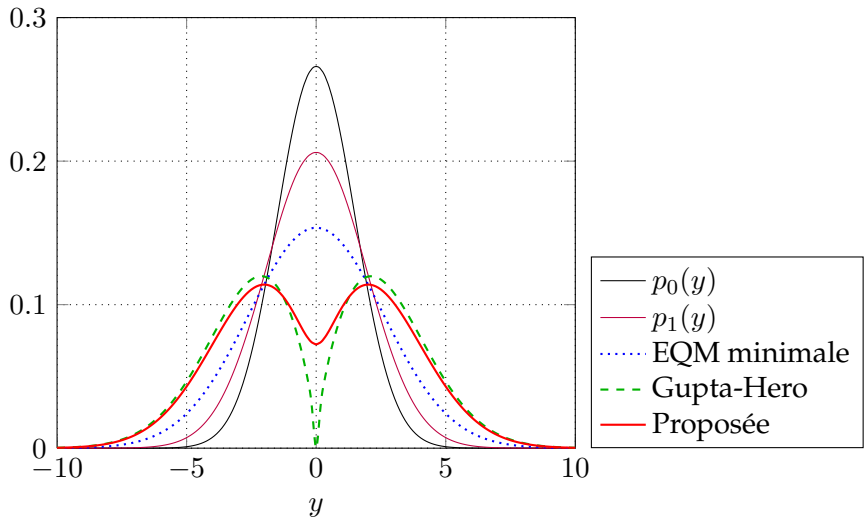


Figure 4.6 – Détection d'un processus MA – Densités de probabilité et densités limites des quantificateurs ($h = [1.06677, -0.59281, 0.09565]$, $\sigma = 1.5$).

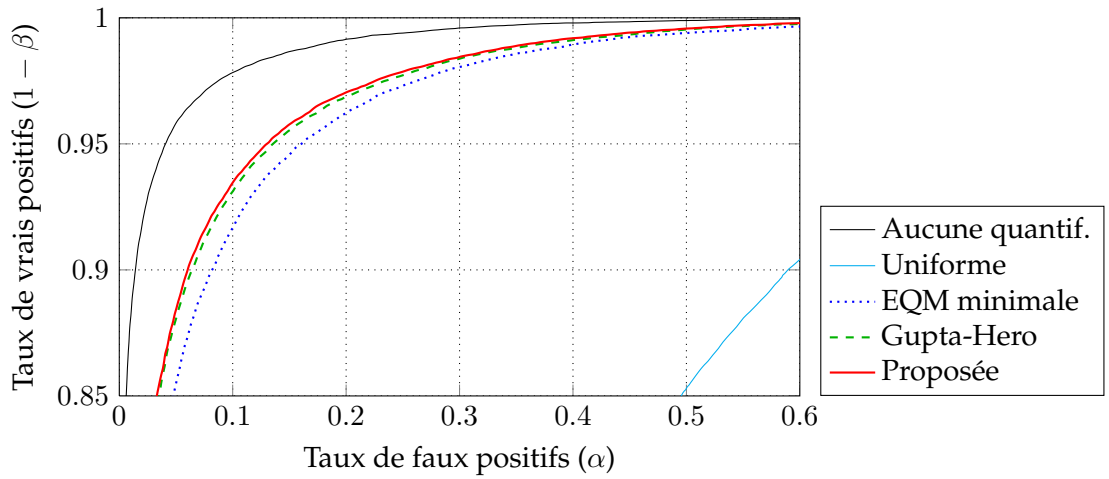


Figure 4.7 – Détection d'un processus MA – Courbes ROC
($h = [1.06677, -0.59281, 0.09565]$, $\sigma = 1.5$, $n = 80$, $N = 4$, 100 000 échantillons).

mais, de même que dans les exemples gaussiens de [61, Section V], nous pouvons toujours calculer le quantificateur correspondant [61, Eq. (25)].

Les performances du test dépendent de la variance du bruit et des valeurs particulières des coefficients du canal. Nous supposons donc que ces coefficients $h_0, \ldots, h_L$ sont des variables i.i.d. gaussiennes centrées réduites, et réalisons plusieurs simulations.

La figure 4.6 représente les différentes densités de probabilité et densités limites pour une certaine réalisation du canal ($h = [1.06677, -0.59281, 0.09565]$) et $\sigma = 1.5$.

Considérons à présent un système composé de $n = 80$ capteurs. En construisant les quantificateurs à 4 cellules et en calculant les distributions quantifiées correspondantes (sous chacune des hypothèses), nous pouvons comparer les différentes méthodes de quantification en termes de performances de détection, via leurs courbes ROC respectives. La figure 4.7 représente ces courbes pour la réalisation du canal ci-dessus. Le quantificateur uniforme est défini sur $[-10\sigma\,;10\sigma]$. Les courbes sont obtenues à partir de $50\,000$ échantillons de LRV sous chaque hypothèse.

La règle de quantification proposée présente les meilleures performances. Dans cet exemple, celles-ci sont proches de celles du quantificateur de Gupta-Hero. Rappelons cependant que ce dernier n'est pas défini dans d'autres contextes (voir les sections 4.7.1 et 4.7.2).

4.8 Conclusion

Dans ce chapitre, nous avons étudié les performances du test de Neyman-Pearson réalisé sur une version quantifiée d'un processus stationnaire corrélé à valeurs vectorielles. Il a été montré que, pour un niveau de fausse alarme fixé, la probabilité de manque de ce test converge exponentiellement vers zéro. Nous avons déterminé l'exposant d'erreur

correspondant et donné une expression compacte de ce dernier dans le contexte de la quantification haute-résolution. En particulier, lorsque le nombre N de points de quantification tend vers l'infini, l'exposant d'erreur converge à la vitesse $N^{-2/d}$ vers celui qu'on obtiendrait sans quantification, où d représente la dimension des observations. Dans le cas scalaire, nous avons caractérisé les quantificateurs haute-résolution qui minimisent la perte en exposant d'erreur. Dans le cas vectoriel, nous avons proposé une méthode basée sur l'algorithme LBG permettant de construire des quantificateurs performants.

Nous pensons que ces résultats peuvent être étendus de différentes manières. Dans ce chapitre, les observations ont des distributions de probabilité absolument continues par rappport à la mesure de Lebesgue ; à la suite de Graf et Luschgy [53, Section 6], nous pourrions considérer des mesures possédant également une partie singulière. De plus, nous avons étudié le comportement asymptotique de chaque point de la courbe ROC (avec un taux de fausse alarme fixé) ; en suivant les raisonnements de [7, 61] et en utilisant les résultats de [27, Section III], il serait intéressant d'étudier la courbe complète et d'utiliser un critère de performance global, comme « l'aire sous la courbe ». Ceci nécessite cependant une extension non-triviale du théorème de Sanov [35] aux processus non-i.i.d.

CHAPITRE 5

Conclusion

5.1 Commentaires généraux

Dans cette thèse, nous avons démontré des résultats fondamentaux sur le codage pour les transmissions sécurisées avec information adjacente aux récepteurs (dans les chapitres 2 et 3), et le codage pour la détection (dans le chapitre 4). En particulier, de nouveaux résultats d'optimalité (caractérisations *single-letter* des régions atteignables) ont été énoncés dans les chapitres 2 et 3, montrant comment utiliser au mieux les caractéristiques du système (informations adjacentes et canaux) pour se protéger contre un espion. Dans le chapitre 4, des conditions légères garantissant la convergence de l'exposant d'erreur du test de Neyman-Pearson dans le régime de la quantification haute-résolution ont été données. Nous pensons que ces résultats, ainsi que les techniques utilisées, peuvent être appliqués et étendus à de nombreux autres problèmes (voir les sections 5.2 et 5.3).

Les limitations de nos résultats viennent principalement du fait que les problèmes étudiés incluent dans leurs définitions certains autres problèmes connus, toujours non résolus. Par exemple, le contexte général du codage de source à plusieurs terminaux sous contrainte de sécurité, considéré dans le chapitre 2, peut être vu comme une extension du problème de Berger-Tung. Celui-ci est toujours ouvert : les meilleurs résultats connus donnent uniquement, dans le cas général, des bornes intérieures et extérieures qui ne coïncident pas. Il en est bien sûr de même pour le problème considéré dans cette thèse.

Dans le chapitre 3, nous avons étudié le problème plus général de la transmission sécurisée d'une source via un canal bruité. Dans cette situation, même si l'intuition semble indiquer que le principe de séparation devrait être satisfait, il n'est pas sûr que ce soit toujours vrai. Nous avons effectivement démontré dans plusieurs cas qu'un schéma séparé est optimal, mais également proposé une stratégie hybride analogique/numérique, optimale dans un exemple gaussien. Le cas général constitue donc un problème ouvert.

Dans le chapitre 4, la connaissance de l'expression asymptotique de la perte en exposant d'erreur introduite par la quantification s'est révélée insuffisante pour concevoir la meilleure stratégie dans le cas vectoriel. L'expression finale implique en effet le profil limite de la famille de quantificateurs considérée, une quantité asymptotique qui définit la forme des cellules. L'ensemble des matrices admissibles en tant que profils limites est inconnu [54], et nous pouvons donc uniquement construire des quantificateurs localement optimaux (c'est-à-dire optimaux dans une certaine sous-classe).

En dépit des limitations indiquées ci-dessus, les travaux de cette thèse peuvent être étendus dans de nombreuses directions. Quelques unes sont identifiées ci-dessous.

5.2 Transmissions sécurisées

Notons tout d'abord que les résultats du chapitre 2 ont déjà inspiré quelques nouveaux résultats. Récemment, la région $\mathcal{R}_{\text{nc}}^*$ a été étudiée dans le cas où la source et les informations adjacentes sont des variables gaussiennes multivariées [41]. À partir de la caractérisation du théorème 2.6 et pour un niveau de distorsion D fixé, une borne extérieure à l'ensemble des débits R et pertes d'information I_e atteignables est démontrée. Il est de plus montré que cette borne est optimale à la limite $R \to \infty$.

À la suite de récents travaux sur le *codage de source avec distributeur d'information adjacente* [126], une extension du théorème 2.6 aux informations adjacentes contrôlées a également été proposée [77]. Dans ce contexte, une suite d'actions T^n est générée à partir du message à débit limité J, avec un certain coût $\Lambda(T^n)$, pour influencer l'information adjacente de chacun des récepteurs. Alice doit alors garantir, en plus des contraintes de distorsion à Bob D, de débit de transmission R_A, et d'incertitude à Ève Δ, que le coût moyen ne dépasse pas un certain seuil P. Une caractérisation *single-letter* de l'ensemble des quadruplets atteignables (R_A, D, P, Δ), est démontrée.

À partir des résultats du chapitre 2, on peut également penser à une extension du problème dit du CEO (pour *Chief Executive Officer*) [13, 43], en y ajoutant des contraintes de sécurité. Dans le problème du CEO classique, L agents observent des versions bruitées d'une variable aléatoire commune cachée. Chaque agent peut communiquer une version compressée de son observation au CEO via un lien à débit limité. Ce dernier souhaite estimer la source cachée, en vérifiant une certaine contrainte de distorsion. Dans sa formulation générale, ce problème est ouvert, mais il est résolu dans certains cas particuliers [120, 121]. La sécurité pourrait être introduite dans ce modèle en considérant qu'un (ou plusieurs) agent est corrompu, celui-ci étant capable d'écouter les communications entre quelques agents voisins et le CEO. Les stratégies de codage mises en place par les agents ont alors pour but supplémentaire de limiter l'information qui « fuite » en direction de cet espion.

D'une manière plus générale, nous pensons que l'approche présentée dans les chapitres 2 et 3 peut être adaptée aux divers contextes de communication impliquant de multiples sources et destinations (par ex., canal à relais, canal à accès multiple, etc.). En particulier, il paraît intéressant d'introduire plusieurs adversaires, afin de prendre en compte le fait que l'émetteur n'a qu'une connaissance imparfaite des informations que possède l'adversaire réel.

Outre les problèmes de communication ci-dessus, des contraintes de sécurité similaires apparaissent dans de nombreux domaines. Par exemple, les gestionnaires de *bases de données* (contenant des données médicales, les préférences de clients, etc.) souhaitent rendre publiques certaines entrées de ces bases, tout en garantissant une certaine confidentialité des individus concernés. Actuellement, les données sont simplement *anonymisées* (le nom et quelques autres champs sensibles sont effacés). Cette procédure est cependant hautement faillible (c'est-à-dire qu'il est possible de renommer les données, et ainsi obtenir des informations confidentielles) dans la mesure où d'autres données, corrélées

à celles-ci, peuvent être disponibles par ailleurs [114, 115]. Pour étudier ce genre de situations d'un point de vue théorique, un cadre général pour la confidentialité et l'utilité dans les bases de données a récemment été proposé [137]. Ce problème et celui du codage de source sous contrainte de sécurité sont certes différents, mais aussi d'une certaine manière reliés [137, Theorem 1]. À mesure que la quantité de données stockées, analysées et partagées (via les réseaux sociaux, les *smartphones*, ou les compteurs électriques intelligents) croît, il paraît crucial de disposer de résultats solides permettant de garantir leur confidentialité.

5.3 Quantification haute-résolution

L'approche développée dans le chapitre 4 pour la quantification haute-résolution adaptée à la détection de processus corrélés peut également être utiles dans d'autres contextes. Par exemple, dans les problèmes d'estimation de paramètres, on peut étudier le comportement asymptotique de l'information de Fisher, qui donne un minorant de la variance de tout estimateur, via la borne de Cramér-Rao [75]. Si les observations sont scalaires et i.i.d., [129, Section III-C] donne la perte asymptotique (dans le régime des hautes résolutions) introduite par une quantification uniforme.

Des travaux en cours [15] ont pour but l'étude de la quantification adaptative pour l'inférence statistique, en étendant tout d'abord ce résultat aux estimateurs récursifs *en ligne* de paramètres *vectoriels*. Dans le cas d'une méthode du gradient stochastique, il est montré que la perte due à la quantification (dans le régime des hautes résolutions) dépend uniquement de la densité et du profil limites de la famille de quantificateurs considérée. Celle-ci dépend cependant des paramètres (évidemment inconnus dans ce problème d'estimation) et ne peut donc être minimisée par avance. L'idée est alors d'apprendre le « bon » quantificateur de manière adaptative en utilisant un algorithme récursif [168].

Les performances des méthodes de détection et d'estimation sont d'une manière générale contrôlées par des termes de la forme $\mathbb{E}[\log p]$ (pour une certaine densité p), comme ceux étudiés dans le chapitre 4. Les techniques utilisées dans cette thèse pourraient donc être appliquées à d'autres problèmes d'inférence statistique, du moment qu'ils font apparaître de telles quantités. C'est par exemple le cas pour l'estimation de l'ordre d'un modèle de Markov caché à états finis [23, 46]. D'autre part, la f-divergence généralisée et la perte correspondante introduite par une quantification scalaire uniforme ont été étudiées dans [129]. Les résultats obtenus s'appliquent aux tests d'hypothèse (via la divergence de Kullback-Leibler [81] ou la distance de Bhattacharyya [14]), à l'estimation de données (via l'erreur quadratique moyenne) et à l'estimation de paramètres (via l'information de Fisher, comme indiqué ci-dessus), pour des processus scalaires i.i.d. L'extension de cette f-divergence généralisée (et des résultats associés) aux processus *corrélés* à valeurs *vectorielles* en utilisant les techniques présentées dans cette thèse paraît prometteuse, tant sur le plan théorique que pratique.

Part II

Task–Oriented Source Coding: Secure Transmission, Detection

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AEP	Asymptotic Equipartition Property
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CSIT	Channel State-Information known at the Transmitter
DD	Decision Device
i.i.d.	independent and identically distributed
LBG	Linde-Buzo-Gray
LLR	Log-Likelihood Ratio
MSE	Mean Square Error
NP	Neyman-Pearson
OSI	Open Systems Interconnection
p.d.f.	probability density function
PCM	Pulse-Code Modulation
ROC	Receiver Operating Characteristic
WSN	Wireless Sensor Network

CHAPTER 1

Introduction

1.1 Preliminaries

In the late XIXth century, the first (analog) data transmission on radio waves was performed (attributed to Tesla, Marconi, and Popov, who all claimed the invention of *radio*), applying the theory of electromagnetic waves developed by Maxwell in 1865 to convey information between two antennas. At the beginning of the XXth century, digital communication techniques appeared, including analog-to-digital conversion (i.e., sampling and quantization of continuous signals, mapping one range of values to one discrete symbol), as well as digital modulation (i.e., transmission of digital information on analog signals, mapping one symbol to one specific waveform). Putting these two basic blocks together enables transmission of analog signals on a wireless medium (e.g., radio waves in the air), through a digital interface, improving both reliability and resource consumption [133]. The first such digital technique, called pulse-code modulation (PCM), was patented by Reeves in 1938. Emergent signal processing and filter theory then provided key tools to design devices with attractive performance.

At the same time, probability and statistics found a new impetus with the development of measure theory [16], led by Borel, Lebesgue, and Radon, among others. It provided the building blocks for Kolmogorov's axiomatisation of probability theory [79] (who later stated many major results on stochastic processes). Numerous models for stochastic processes (e.g., Markov chains) were also proposed, along with tools for their analysis, including the general ergodic theory, which is concerned by the limiting behavior (e.g., as time goes to infinity) of dynamical systems [159]. Statisticians found in this theory fundamental tools for modern statistical inference, including detection [87] and estimation [86] theories. Roughly speaking, statistical inference is interested in drawing a conclusion on a system from an experiment. Usually, the experiment produces samples of data that are modeled by some stochastic process; the decision then concerns this model. For instance, parameter estimation is interested in finding the value of the parameters of the model that best *explain* the observed data; detection is interested in deciding between several possibilities (the *hypotheses*) e.g., detecting a target in a region under surveillance with radar signals [142].

Gathering the physics of electromagnetic radiation, and the above mathematical constructions, stochastic *source* and *channel* models were developed in the context of telecommunications. The randomness in these models reflects the facts that transmitted data are unknown while designing a communication device, that the wireless medium (i.e., the

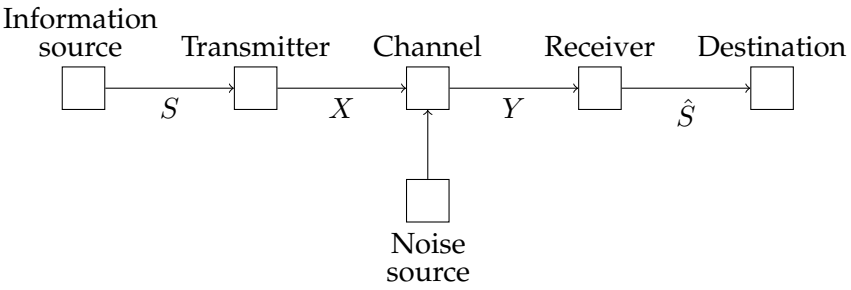


Figure 1.1: Schematic diagram of a general communication system [139].

air) is complex, time-varying, and full of electromagnetic radiations (natural ones or interfering signals from other systems), and that electronic components produce additional thermal noise. In 1948, Shannon presented his pioneering *mathematical theory of communications* [139], which aimed to provide a general model for information processing and transmission, as well as some fundamental results. In this framework, as depicted in Figure 1.1, a communication system is composed of

- an information source, that produces messages represented by some random variable S which takes values on some set $\mathcal{S}$,
- a transmitter, that processes the message S, and sends some signal X over the medium,
- a channel $X \mapsto Y$, represented by some transition probability $p(y|x)$ i.e., the probability of receiving y when x is sent,
- a receiver, that computes a reconstruction $\hat{S}$ of the message S from the received signal Y,
- a destination, for which the message is intended.

This construction enables *theoretical* analysis of a given communication system, which will further provide communication engineers with fundamental limits to compare their practical methods and devices with.

Focusing on discrete systems, Shannon used the *entropy* as a measure of information (or uncertainty) for random sources, defined for some source S as

$$H(S) = -\sum_{s \in \mathcal{S}} p(s) \log p(s) \ ,$$

where, for each $s \in \mathcal{S}$, $p(s)$ is the probability of the event $\{S = s\}$. His main results state that the performances of communication systems are somehow ruled by quantities of that kind. In particular, Shannon proved that reliable transmission of a source S can take place at rate R if and only if its entropy $H(S)$ is below R. For the transmission over a noisy channel $X \mapsto Y$, this rate should be below the so-called *capacity*, given by the following equation:

$$C = \max_{p(x)} I(X;Y) \ ,$$

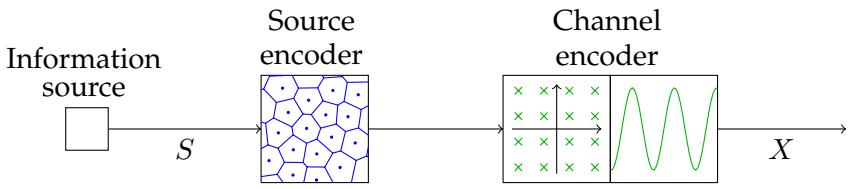


Figure 1.2: A separated transmitter.

where $I(X;Y)$ is the *mutual information* between the input and the output [31]. The main idea of the proof is to simultaneously allow a small fraction of errors and a large number of transmissions. This enables to send redundancies (roughly speaking, repetitions) which will help to average the noise of the channel and eventually identify the sent message.

The key tools for analyzing (abstract) *codes* i.e., transmitter and receiver strategies, are the so-called *random coding* argument and *typical sequences*, which deal with the asymptotic properties of random sequences, as their length tends to infinity. The basic result in Shannon's proof, namely the *asymptotic equipartition property* (AEP), was extended to general ergodic processes, yielding the so-called Shannon-McMillan-Breiman theorem [21, 104], further generalized in many ways [6, 110] (see also [51] for a review of the different generalizations and extensions). These results then led to coding theorems for more general systems [162] e.g., systems with memories, continuous systems.

As a consequence, Shannon proved that it is *optimal* to separately compress the source (*source coding*) and then represent the compressed data in a fashion adapted to the channel (*channel coding*), as depicted in Figure 1.2. In other words, sending analog signals on a wireless medium through a digital interface (as done in the early years of digital communications) is the best strategy.

During the same period, considerable attention was paid to the development of a *quantization theory* for continuous signals (see [53, 54]). In 1948, Oliver, Pierce, and Shannon [118] thoroughly analyzed PCM, and provided an approximation of the *average* distortion introduced by a uniform quantizer when the number of bits tends to infinity. This *high-resolution* analysis was later extended to *companders* [8, 122]. Such systems are composed of a "compressor" (an invertible function ϕ) followed by a uniform quantizer; the reconstruction is obtained after an expansion step, that inverses the compressor i.e., that applies ϕ^{-1} (see Figure 1.3). In particular, the so-called *Bennett's integral* [8, Eq. (1.6)] gives the asymptotic mean square error (MSE) for a compander compressing a source S into reconstruction $\hat{S}_N$, as the number of quantization levels N tends to infinity:

$$\mathbb{E}\left[\left(\hat{S}_N - S\right)^2\right] \approx \frac{1}{12N^2} \int \frac{p(s)}{[\phi'(s)]^2}\,\mathrm{d}s\,.$$

This result was further generalized to quantizers with *point density*, as well as vector quantizers [111] i.e., quantizers that work on buffered blocks of data. From such asymptotic approximations, researchers derived quantization strategies which would

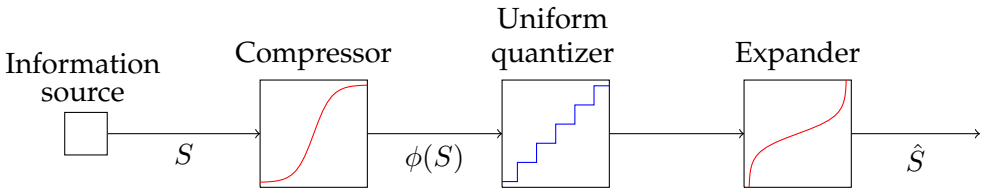


Figure 1.3: A compander.

yield small average distortion for various stochastic source models. Algorithms for practical implementation of these strategies were also developed [93, 99].

Note that in this approach the aim was to design good "stand-alone" quantizers i.e., that would yield a good estimate of the message at the destination, assuming reliable communication of the quantized data between the transmitter and the receiver, as justified by the separation theorem [34, 139].

1.2 Practical communication systems

From these theoretical results, and in order to ease practical developments, *layered* architectures for *general-purpose* systems (as the one depicted in Figure 1.4, and the Open Systems Interconnection (OSI) model [69]) quickly became standard. In such schemes, a specific task is assigned to each layer. In particular, channel coding is performed at the physical layer, and all above layers then assume error-free information. The general idea is to come up with basic blocks that can be separately designed. Advances in one field (e.g., data compression, error correction, modulation, synchronization, channel estimation, medium access control) can then be quickly implemented and benefit all systems. Many modern communication technologies are basically built on such a layered architecture e.g., the Internet (with TCP/IP), or the Universal Mobile Telecommunications System (UMTS).

Considering there are threats that can attack the resources (the information itself or devices that manage it), *security* services are defined for the OSI model [68]. They aim to ensure the so-called *CIA triad* defined as:

- Confidentiality: The information should not be disclosed to unauthorized individuals or systems;
- Integrity: A third party should not alter the data without being detected;
- Availability: The information must be available when it is needed.

These services are not related to a specific layer. Roughly speaking, each layer should care about the security of its own data. In practice, confidentiality is handled through total *encipherment* of the data stream [68], using cryptographic techniques essentially based on computational complexity. Note that security then only depends on the intractability assumption of some hard problems (e.g., factoring large integers).

Putting everything together, layered general-purpose systems, as those currently implemented, yield devices that can eventually be modeled by three successive stages (see also Figure 1.4):

- source coding (or data compression),
- data encryption,
- channel coding.

Each stage is independently designed, regardless of the eventual use of the data. However, the primary results [139] hold for point-to-point communications, when one transmitter wishes to send through a channel with known (and fixed) statistics a compressed version of a local source that must be accurately estimated at one destination, without any security requirement (see Figure 1.1). As a matter of fact, other settings may be much more involved, and have been the focus of intense research for many decades. They include multiterminal compression [9, 143], data compression with side information [4, 155, 166], distributed detection [2, 153] and computation [44, 108], secure transmission under eavesdropping [32, 106, 165]. Many of the above settings are still open in their general statement.

On the other hand, as wireless networks get widely deployed, we now see many limitations in current technologies. For instance, the fast development of mobile Internet access (e.g., through 3G), as well as embedded systems (in airplanes, cars, etc.), calls for a good use of resources e.g., bandwidth; otherwise, operators might face huge congestion problems. Recent advances in electronics moreover enable to produce small devices with limited capabilities that can be massively spread to form a so-called wireless sensor network (WSN) [5, 146]. In practice, WSN are intended to manage production lines, to detect abnormal events and forecast natural disasters, to perform field surveillance, to detect

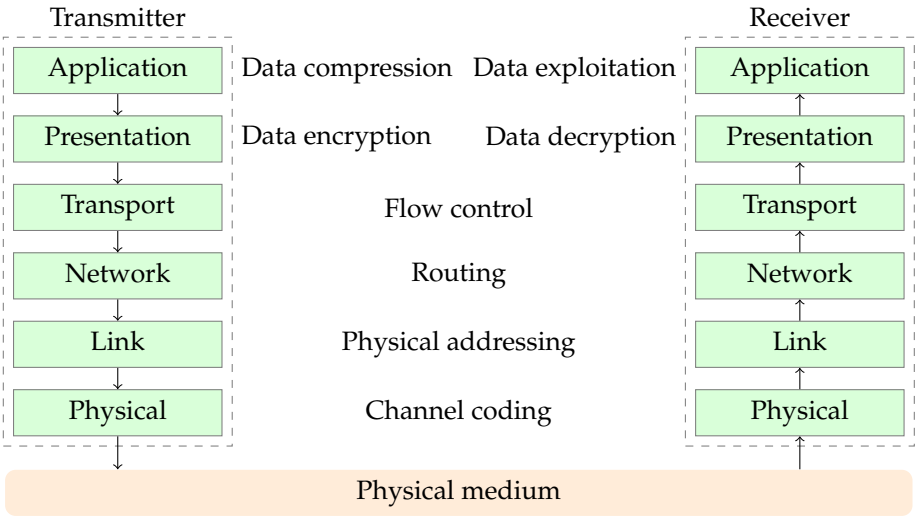


Figure 1.4: A layered architecture and some potential tasks.

and localize targets, etc. [88]. Robot flees also constitute examples of communication systems that operate in severe environments for e.g., space exploration, oil extraction, or rescue operations [22, 92]. Running such multi-agent systems requires the development of *specific* efficient sensing, communication, networking, and signal processing techniques.

1.3 Task-oriented strategies

Considering that the destination does not want so much to *get* the data as to *use* them, *task-oriented* (or *application-driven*) strategies constitute a promising trend for such emergent and future wireless technologies. By designing systems for a particular application, and by relaxing the layered structure (e.g., allowing *cross-layer* optimization), they aim to improve the performances for some given classes of problems. For instance, the management of the quality of service (QoS) should be quite different if the destination wants to download an entire file, or if it wants to watch a live video. Different purposes should yield different ways to measure quality and, more generally, performance. Considering the final use of the processed and transmitted information as the key concern of communication systems, several new concepts have recently emerged e.g., content-centric networking [36], application-oriented routing [145] and architecture [67].

In terms of source coding, this task-oriented perspective has long been considered in a theoretical point of view through the so-called *rate-distortion* theory [10, 34, 141]. In this framework, the destination wants to find an approximate estimate $\hat{S}^n$ of the source sequence S^n from some rate-limited message; the "quality" of the final estimate is measured through the average distortion $\frac{1}{n}\sum_{i=1}^{n} d(S_i, \hat{S}_i)$, where $d\colon \mathcal{S}\times\mathcal{S} \to \mathbb{R}_+$ is a so-called *distortion measure*. For a given rate, the aim of the transmitter is then to find the coding scheme that minimizes the induced distortion. There is obviously a trade-off between the allowed rate and distortion level, which is summarized by the *rate-distortion* function $R(D)$, defined as the minimum rate enabling a distortion level of at most D. As a matter of fact, d can be chosen to fit a particular purpose. For instance, several *perceptual* distortion measures have been proposed for audio compression in order to quantify the quality of the compression as felt by a human user. However, other contexts may be hard to include in this general rate-distortion theory, mainly due to the symbol-by-symbol average distortion criterion. New theoretical results are needed in these cases.

In this dissertation, we consider the following problems:

- secrecy-oriented source coding, and
- detection-oriented source coding.

The following paragraphs give some preliminaries as well as an overview of our contributions on these topics. In both cases, we characterize the performances of coding schemes through asymptotic studies to come up with deterministic quantities. Optimizing these quantities yields fundamental limits on the performance of the considered systems, as well as strong guidelines for their practical design.

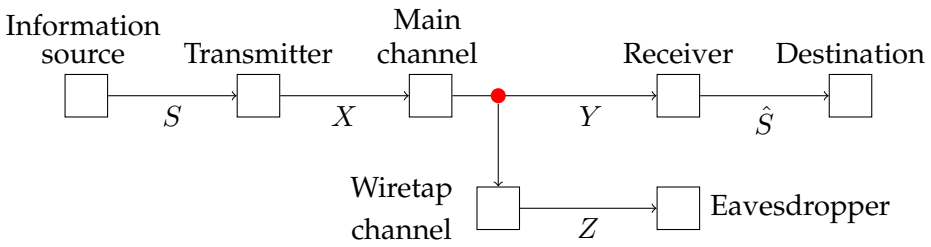


Figure 1.5: The wiretap channel [165].

1.3.1 Secrecy-oriented source coding

Due to the open nature of the wireless medium, wireless communications are very sensitive to *eavesdropping* i.e., when an adversary listens to the exchanged messages. On the other hand, the intrinsic randomness of sources and channels can provide additional security while advantageously used. In order to include such settings in the general framework of communication systems [139], Shannon introduced the information-theoretic notion of secrecy, where security (more precisely, confidentiality) is measured through the equivocation –the remaining uncertainty about the message– at the eavesdropper [140]. As it only relies on the statistical properties of the system, this approach ensures unconditionally (regardless of the eavesdropper's computing power and time) secure schemes. In particular, they cannot be broken by brute force.

Since then, researchers have investigated many settings for secure communication. As a matter of fact, almost all traditional problems have been extended to consider additional security constraints. In terms of channel coding, Wyner introduced the *wiretap channel* [165], where the channel of the eavesdropper ($X \mapsto Z$) is a degraded version of the legitimate user's one ($X \mapsto Y$) (see Figure 1.5), and showed that it is possible to send information at a positive rate with perfect secrecy, up to the *secrecy capacity* C_s defined as

$$C_s = \max_{p(x)} I(X;Y|Z) \ .$$

In such a case, the eavesdropper cannot retrieve any information from the communication. Roughly speaking, the messages are made almost uniform by additional digital random noise (introduced at the transmitter) and by the wiretap channel, so that the eavesdropper will never be able to identify which ones were sent [18].

This model has called extensive research on theoretical and practical aspects of the so-called *physical-layer security* [1, 90, 95], which provides new mechanisms for securing transmissions that are not included in the original OSI model [68]. While these techniques introduce security requirements at the channel coding step, fewer results have been reported on secure source coding.

Following Shannon's definition of information-theoretic security [140], the equivocation at the eavesdropper (about the source) can be used besides the distortion level at the legitimate receiver to measure the overall performance of source coding strategies. For

a given rate, the aim of the transmitter is now to find the coding scheme that minimizes the induced distortion while also maximizing this equivocation. In this approach, secrecy requirements are directly taken into account at the data compression stage. While it implies a similar trade-off, this framework cannot be directly included in the rate-distortion theory: The equivocation cannot be written as a symbol-by-symbol distortion measure. A new dimension for secrecy requirements should thus be added to the classical rate-distortion setup.

This thesis (in Chapters 2 and 3) provides some new fundamental results on *secrecy-oriented* source coding in the presence of side informations at the receiving terminals. More precisely, in Chapter 2, we investigate the problem of *secure multiterminal source coding with side information at the eavesdropper*. This scenario consists of four nodes:

- a main encoder (referred to as Alice), that observes a local source,
- a legitimate receiver (referred to as Bob), that wishes to estimate Alice's source from a compressed version received through a (public) rate-limited link,
- a second encoder (referred to as Charlie), that helps Bob in estimating Alice's source by sending a compressed version of its own correlated observation via a (private) rate-limited link,
- an eavesdropper (referred to as Eve), that perfectly observes the information bits sent by Alice to Bob, and has also access to a correlated source which can be used as side information.

For instance, this scenario can occur in a WSN context: Alice and Charlie then represent legitimate sensors, Eve a "hacked" sensor, and Bob a remote user that wants to be informed about Alice's environment while keeping Eve as ignorant as possible. In this setting, Alice wants to simultaneously satisfy the desired requirements on the distortion level at Bob and the equivocation at Eve. Fundamental results on the corresponding achievable region are derived. In particular, *optimal* coding schemes are characterized for some cases of interest where the properties of the system can be fully exploited for secrecy.

In Chapter 3, we partially extend the results of Chapter 2 considering noisy channels between the main encoder –Alice– and the receivers –Bob and Eve. In this problem of *secure transmission of sources over noisy channels with side informations*, Charlie and Bob are now collocated, and Alice still aims to simultaneously satisfy distortion and security requirements, taking advantages of sources and channels at the same time. As a matter of fact, it is not clear if the findings of Chapter 2 together with the ones on the wiretap channel [32, 165] would yield good performance. In this dissertation, we provide fundamental results on the so-called *rate-distortion-equivocation region*. Novel digital and hybrid digital/analog schemes are proposed in this setting.

1.3.2 Detection-oriented source coding

In a detection problem, a user would like to identify which situation it is facing (among several possible ones), based on the observation of some signal. In case of two possible hypotheses, $\mathsf{H}0$ –in a radar context, the region under surveillance is clear– and $\mathsf{H}1$ –a target is present, its decision can be wrong in two manners. Either it decides that the received samples come from the distribution corresponding to hypothesis $\mathsf{H}1$ while the true one is $\mathsf{H}0$ (*false alarm*), or it decides $\mathsf{H}0$ instead of $\mathsf{H}1$ (*missed detection*). The probabilities of these two events, respectively denoted by α and β, together give the performance of a detector (or a test). As as matter of fact, there is a trade-off between α and β that can be visualized through the so-called *receiver operating characteristic* (or ROC curve), that plots $1-\beta$ as a function of α [76]. Under some assumptions, the ROC curve converges to constant 1 (which corresponds to a perfect detector) at an exponential speed, as the number n of received samples tends to infinity:

$$\beta \simeq \exp(-n\,K),$$

where K is the rate of convergence, independent of α, referred to as the *error exponent*. This quantity is a key metric for designing tests that will eventually yield good practical (i.e., for some finite n) performance.

If the user is far from the phenomenon of interest, it may receive the data from some remote sensor. These two devices then form a communication system as in Figure 1.1. For a given rate, the aim of the transmitter is now to find the coding scheme that maximizes the error exponent. If the samples are independent and identically distributed (i.i.d.) under each hypothesis, the latter corresponds to the Kullback-Leibler divergence between the distributions under $\mathsf{H}0$ and $\mathsf{H}1$ [81]. However, the classical rate-distortion theory does not apply here: The error exponent cannot be written as a traditional distortion measure.

This thesis (in Chapter 4) investigates some theoretical aspects of *detection-oriented* quantization. Assuming that the source can be modeled by some stationary ergodic multivariate process, we follow the approach of [61, 111] to investigate the effect of quantization on the performance of the Neyman-Pearson test. The main contribution is to provide a compact expression of the corresponding *error exponent* in the so-called *high-rate* regime i.e., when the number of quantization levels tends to infinity. This result can be viewed as the equivalent of Bennett's integral [8] in this particular setup of the detection of multivariate correlated processes. It is valid under some mixing conditions on the observed process, as well as assumptions on the limiting behavior of the quantizers in the high-rate regime. As an application, relevant detection-oriented quantization strategies are determined.

CHAPTER 2

Secure Multiterminal Source Coding with Side Information at the Eavesdropper

Abstract. In this chapter, we investigate the problem of secure multiterminal source coding with side information at the eavesdropper. This scenario consists of a main encoder that wishes to compress a single source, simultaneously satisfying the desired requirements on the distortion level at a legitimate receiver and the equivocation rate at an eavesdropper. It is assumed the presence of a rate-limited link between the encoder and the two receivers. The legitimate receiver is furthermore helped by a second encoder that sends a compressed version of its own correlated observation via a (private) rate-limited link. Moreover, the eavesdropper has access to a correlated source which can be used as side information. For instance, the problem at hands can be seen as the unification between the Berger-Tung and the secure source coding setups. Inner and outer bounds on the so called rates-distortion-equivocation region are derived. The inner region turns out to be tight for two special cases. The statistical differences between the side information at the decoders, and the presence of a non-zero distortion can thus be fully exploited in terms of secrecy. Application examples to secure lossy source coding of Gaussian and binary sources in the presence of Gaussian and binary/ternary (resp.) side informations are also considered.

2.1 Introduction

Consider the classical problem of compressing a source at a sensor node (referred to as Alice) which must be estimated at a remote destination (referred to as Bob) within a certain distortion level. Assume also that a (public) rate-limited link is available between the two devices. In addition to this, the encoder wishes to leak the least possible amount of information about its source to an eavesdropper (referred to as Eve) e.g., an untrusted sensor, who perfectly observes the information bits sent by Alice and may have access to an observation correlated to the source. Another sensor (referred to as Charlie) will help Bob in estimating Alice's source by sending a compressed version of its own correlated observation on a (private) rate-limited link, which is only observed by Bob. In this setting, the correlation between the observations can be useful not only to decrease the rate needed for the communications, but also to increase secrecy, which means the average uncertainty of Eve about Alice's source. From a theoretical viewpoint, the problem

at hands is therefore very rich and still quite open, as it contains, as subproblems, the long-standing information-theoretic problem of distributed lossy source coding, as well as recent ones e.g., source coding with security constraints.

Slepian and Wolf [143] introduced the problem of distributed lossless compression i.e., when Bob wants to perfectly estimate both sources of Alice and Charlie. Wyner [163] and Ahlswede and Körner [4] characterized the achievable region when only one source is to be estimated i.e., source coding with coded (or partial) side information. Generalization of the Slepian-Wolf setup to arbitrary distortion levels on both sources was introduced by Berger [9], who provided inner and outer bounds on the achievable region which do not match in general. When Bob is intended to estimate only one source, Berger et al. [11] provided a new inner bound which was further proved in [70] to be equivalent to the one of [9], and strictly sub-optimal [157]. Several results of optimality were proved in case of uncoded side information [166], lossless reconstruction of at least one source [12], and in some special cases, including Gaussian sources with quadratic distortion measure [119, 158]. Over the years, these topics have been the focus of intense study and some remarkable progress has been made in theoretical and practical aspects, including general frameworks for lossless compression with multiple terminals [33, 63], lossy source coding with uncertain side information at the decoder [66, 73], lossy compression with partially separated encoders [72] or with many decoders [150–152], some results of optimality for Gaussian sources in various contexts [134, 148], as well as the design of nested codes for distributed compression e.g., using parity-check [174], lattice [98, 138, 174], or algebraic trellis [132] codes. Nevertheless, in spite of these efforts, the simplest scenario of distributed lossy compression first introduced in [9] still remains open.

On the other hand, extensive research has been done on secure communication. The traditional focus was on cryptography, based on computational complexity where security only depends on the intractability assumption of some hard problems. Shannon in [140] introduced the information-theoretic notion of secrecy, where security is measured through the equivocation rate –the remaining uncertainty about the message– at the eavesdropper. This information-theoretic approach of secrecy allows to consider security issues at the physical layer, and ensures unconditionally (regardless of the eavesdropper's computing power and time) secure schemes. Adopting this approach in a channel coding perspective, Wyner introduced the wiretap channel in [165] and showed that it is possible to send information at a positive rate with perfect secrecy as long as the channel of the eavesdropper is a degraded version of the legitimate user's one. Csiszàr and Körner [32] extended this result to the setting of general broadcast channels with any arbitrary equivocation rate. Since then, several extensions have been proposed e.g., for fading channels [89], arbitrary i.e., not necessarily stationary memoryless, channels [17], channels with state information at the encoder [28], cooperative relay broadcast channels [40] (see also [1, 90, 95] for a review of recent results), as well as practical coding schemes for secure communication e.g., nested codes for (Gaussian and binary) type-II wiretap channels [96], LDPC [78] and lattice [117] codes for the Gaussian wiretap channel,

polar codes for binary symmetric channels [101], and construction of secure codes from ordinary channel codes [65]. So far, very few work has been reported on source coding problems with security constraints, while early work [3,103] showed that the presence of correlation between different observations may guarantee some secrecy.

Researchers have employed two approaches in the literature of secure source coding. In fact, it is assumed either that there already exists a secure rate-limited link between Alice and Bob, which allows the system to use secret keys, or at least the decoders have access to some side information about the source. In the scenario of secret key sharing, both lossless and lossy compressions have been studied in various contexts [105,169–172]. Classical lossy source coding followed by encryption using the secret key was proved to be optimal when the receivers have no side information [172]. For the second scenario, recent work [131] considered the case of lossless source coding with (uncoded) side information at both decoders under the assumption of no rate constraint in the communication between Alice and Bob. In such a case, the usual Slepian-Wolf scheme is proved to be insufficient. Lossless source coding with coded side information, resp. distributed lossless compression, has been studied in [56,147], resp. [55]. In their "one-sided helper" scenario, the authors of [147] characterized the achievable region when only one source is to be perfectly estimated and Eve does not have any side information. In particular, they proved that the scheme of Wyner [163] and Ahlswede and Körner [4] achieves the whole region. Inner and outer bounds on the achievable region for secure distributed lossless compression have been proposed in [55]. Secure *lossy* source coding with side information at the decoders received less attention. As a matter of fact, if the (uncoded) side informations at the decoders are degraded then the achievable region can be derived as a special case of [106] where Wyner-Ziv coding [166] is optimal.

In this chapter, we investigate the general problem of secure lossy source coding of memoryless sources with coded side information at the legitimate receiver in the presence of an eavesdropper, who in addition to observe the information bits can also have access to correlated side information, as depicted in Figure 2.1. It is assumed that all links between encoders and decoders are noiseless so that they cannot provide any advantage to increase secrecy. This setting can be seen as the natural extension of the Berger et al. problem [11] to the one with security constraints. We provide inner and outer bounds on the achievable region, referred to as the *rates-distortion-equivocation region*. These bounds do not match in general because of a long Markov chain condition, as in [9,11]. From the proposed inner region, we derive two results of optimality for the cases of: (*i*) uncoded side information, generalizing the results in [56,131] to any arbitrary distortion level, and (*ii*) lossless reconstruction of both sources at the legitimate receiver (i.e., distributed lossless compression), refining [55]. When dealing with the lossy case in the presence of uncoded side information, it should be mentioned here that if one side information (either at Bob or Eve) is less noisy than the other, then Wyner-Ziv coding is sufficient. Similarly, for the distributed lossless compression setting it is shown that if the side information at Eve is less noisy than the observation of Charlie, then Slepian-Wolf coding achieves the whole region. As an application example, we consider the case of secure lossy source

coding of a Gaussian source with Gaussian side informations, extending [119] to the scenario with security constraints. We also consider the case of secure lossy source coding of a binary source, where the (uncoded) side information at Bob (resp. Eve) is the output of a binary erasure channel (resp. a binary symmetric channel) with the source as the input. This model is of theoretical interest since neither Bob nor Eve can always be a less-noisy decoder.

The rest of this chapter is organized as follows. Section 2.2 states definitions along with the main results on secure lossy source coding with coded side information at the legitimate receiver i.e., inner and outer bounds on the rates-distortion-equivocation region. The proof of the inner bound is given in Section 2.3. Section 2.4 (resp. Section 2.5) provides an optimal characterization of the achievable region for the case of uncoded side information at Bob (resp. distributed lossless compression). Section 2.6 presents application examples to Gaussian and binary sources. Finally, Section 2.7 summarizes the chapter.

Notation

For any sequence $(x_i)_{i\in\mathbb{N}^*}$, notation x_k^n stands for the collection $(x_k, x_{k+1}, \ldots, x_n)$. x_1^n is simply denoted by x^n. Let $\mathcal{T}$ be an arbitrary finite set. The cardinality of $\mathcal{T}$ is denoted by $\|\mathcal{T}\|$. For any subset $\mathcal{S} \subseteq \mathcal{T}$, notation $\mathbf{1}_{\mathcal{S}}$ stands for the indicator function of $\mathcal{S}$ in $\mathcal{T}$ i.e., for each $t \in \mathcal{T}$, $\mathbf{1}_{\mathcal{S}}(t) = 1$ if $t \in \mathcal{S}$, and $\mathbf{1}_{\mathcal{S}}(t) = 0$ otherwise. Entropy is denoted by $H(\cdot)$, and mutual information by $I(\cdot;\cdot)$. We denote typical and conditional typical sets by $T_\delta^n(X)$ and $T_\delta^n(Y|x^n)$, respectively (see Appendix A for details). Let X, Y and Z be three random variables on some alphabets with probability distribution p. If $p(x|yz) = p(x|y)$ for each x, y, z, then they form a Markov chain, which is denoted by $X \multimap Y \multimap Z$. Random variable Y is said to be less noisy than Z w.r.t. X if $I(U;Y) \geq I(U;Z)$ for each random variable U such that $U \multimap X \multimap (Y, Z)$ form a Markov chain. This relation is denoted by $Y \succeq_X Z$. The set of nonnegative real numbers is denoted by $\mathbb{R}_+$. For each $x \in \mathbb{R}$, notation $[x]_+$ stands for $\max\{0\,;x\}$. Logarithms are taken in base 2 and denoted by $\log(\cdot)$. The binary entropy function is defined on $[0,1]$ as $h_2(x) = -x\log(x) - (1-x)\log(1-x)$. Its inverse h_2^{-1} is defined on $[0,1]$ and takes values in $[0, \frac{1}{2}]$. For each $a, b \in [0,1]$, $a \star b = a(1-b) + (1-a)b$.

2.2 Secure lossy source coding with coded side information

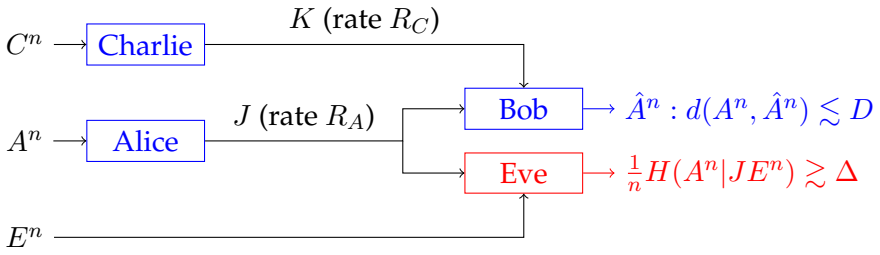


Figure 2.1: Secure lossy source coding with coded side information.

2.2.1 Definitions

In this section, we give a more rigorous formulation of the context depicted in Figure 2.1. Let $\mathcal{A}$, $\mathcal{C}$ and $\mathcal{E}$ be three finite sets. Alice, Charlie and Eve observe sequences of random variables $(A_i)_{i\in\mathbb{N}^*}$, $(C_i)_{i\in\mathbb{N}^*}$ and $(E_i)_{i\in\mathbb{N}^*}$ respectively, which take values on $\mathcal{A}$, $\mathcal{C}$ and $\mathcal{E}$, resp. For each $i \in \mathbb{N}^*$, random variables A_i, C_i and E_i are distributed according to the joint distribution $p(ace)$ on $\mathcal{A} \times \mathcal{C} \times \mathcal{E}$. Moreover, they are independent across time i.

Let $d\colon \mathcal{A}\times\mathcal{A} \to [0, d_{\max}]$ be a finite distortion measure i.e., such that $0 \leq d_{\max} < \infty$. We also denote by d the component-wise mean distortion on $\mathcal{A}^n\times\mathcal{A}^n$ i.e., for each $a^n, b^n \in \mathcal{A}^n$, $d(a^n, b^n) \triangleq \frac{1}{n}\sum_{i=1}^n d(a_i, b_i)$.

Definition 2.1 (Code)**.** An (n, R_A, R_C)-code for source coding in this setup is defined by

- an encoding function at Alice $f_A\colon \mathcal{A}^n \to \{1, \dots, 2^{nR_A}\}$,
- an encoding function at Charlie $f_C\colon \mathcal{C}^n \to \{1, \dots, 2^{nR_C}\}$,
- a decoding function at Bob $g\colon \{1, \dots, 2^{nR_A}\} \times \{1, \dots, 2^{nR_C}\} \to \mathcal{A}^n$.

Definition 2.2 (Achievability)**.** A tuple $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) such that:

$$\mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] \leq D + \varepsilon\,,$$
$$\frac{1}{n} H(A^n|f_A(A^n), E^n) \geq \Delta - \varepsilon\,.$$

The set of all such achievable tuples is denoted by $\mathcal{R}^*$ and is referred to as the *rates-distortion-equivocation region*.

Remark 2.1. Region $\mathcal{R}^*$ is closed and convex.

Remark 2.2. Quantities involved in Definition 2.2 only depend on the marginal distributions $p(ac)$ and $p(ae)$. The same applies for subsequent results that provide inner and outer bounds on $\mathcal{R}^*$.

2.2.2 Inner bound

The following theorem gives an inner bound on region $\mathcal{R}^*$ i.e., it defines region $\mathcal{R}_{\text{in}} \subseteq \mathcal{R}^*$. The proof is based on superposition coding and random binning at the encoders Alice and Charlie, and joint decoding at Bob. The proposed scheme along with standard properties of typical sequences enables to characterize the equivocation rate at Eve.

Theorem 2.1 (Inner bound). *A tuple $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist random variables U, V, W on some finite sets $\mathcal{U}, \mathcal{V}, \mathcal{W}$, respectively, with joint distribution $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, verifying the following inequalities:*

$$R_A \geq I(V;A|W)\,, \tag{2.1}$$

$$R_C \geq I(W;C|V)\,, \tag{2.2}$$

$$R_A + R_C \geq I(VW;AC)\,, \tag{2.3}$$

$$D \geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\,, \tag{2.4}$$

$$\Delta \leq H(A|VW) + I(A;W|U) - I(A;E|U)\,, \tag{2.5}$$

$$\Delta - R_C \leq H(A|V) - I(A;E|U) - I(W;C|V)\,. \tag{2.6}$$

Region $\mathcal{R}_{in}$ is defined as the convex hull of the set of all such tuples.

Proof. See Section 2.3. □

The above inner region can also be achieved using a time-sharing combination of three complementary families of codes. Since this approach may yield better intuition, its proof is sketched below (see the *Sketch of proof* on page 143).

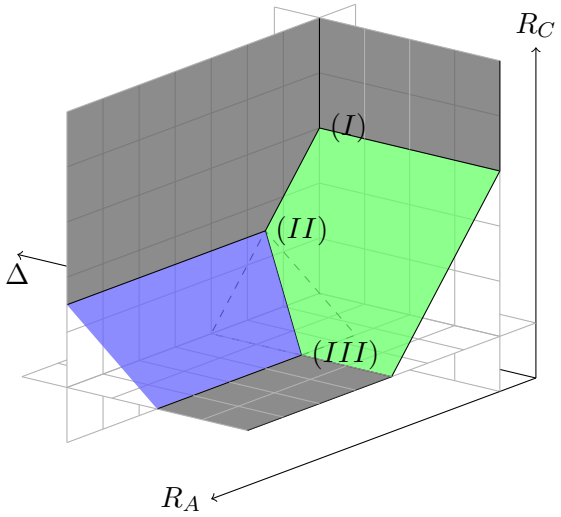


Figure 2.2: Achievable tuples (R_A, R_C, Δ) for some fixed distortion level D.

Inequalities (2.1)–(2.3) are identical to the ones of Berger and Tung [9]. They ensure perfect reconstruction of both variables V and W at Bob, who can hence compute estimate $\hat{A}(V,W)$ of A. The sum-rate constraint (2.3) captures the trade-off between rates R_A and R_C: The information must be transmitted by one or the other encoder.

Let us now give some intuition on (2.5) and (2.6). The first term $H(A|VW)$ corresponds to the equivocation rate at Bob. Alice thus exploits the admissible distortion at Bob to increase the equivocation rate at Eve. Moreover, for given variables V and W, which determine the rates and the distortion level at Bob, the auxiliary variable U can be tuned to make Bob *more capable* than Eve i.e., maximize $I(A;W|U) - I(A;E|U)$. This quantity represents the gain (or the loss) at Eve in terms of equivocation rate. At the same time, (2.6) imposes a trade-off between the equivocation rate at Eve Δ and the rate of Charlie R_C, which captures the fact that Δ cannot be too large if R_C is not: If the secrecy requirement is harsh, more information must be sent through the private link (between Charlie and Bob). We will refer to quantity $\Delta - R_C$ as the *public-link secrecy rate*.

Note that (2.5) also writes

$$\Delta \leq H(A|UE) - I(V;A|UW)\,.$$

Variable U is thus considered as a *common message* i.e., as if Eve could decode it. As a matter of fact, in case of uncoded side information at Bob (resp. distributed lossless compression), Proposition 2.8 (resp. 2.13) shows that it is optimal to encode U so that Eve can reliably estimate it. The remaining information rate of Alice (on the public link) i.e., $I(V;A|UW)$, is directly subtracted from the equivocation rate, meaning that it is treated as "raw" bits of A.

Sketch of proof of Theorem 2.1 (Time-sharing combination technique). We first construct three codes achieving corner points (I), (II) and (III) illustrated in Figures 2.2, 2.3 and 2.4. Each corner point is achieved using a three-step communication scheme which aim is to reliably deliver variables (U,V) and W, descriptions of A at Alice and C at Charlie, respectively, to Bob. Note that V is on the top of U (*superposition coding*). At each step, the information previously received (and decoded) is used as side-information at Bob. *Random binning* a la Wyner-Ziv [166] is performed to take advantage of this side information.

Corner point	(I)	(II)	(III)
Decod. order	W, U, V	U, W, V	U, V, W
R_A	$I(V;A\|W)$	$I(U;A) + I(V;A\|UW)$	$I(V;A)$
R_C	$I(W;C)$	$I(W;C\|U)$	$I(W;C\|V)$
D	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$	$\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$
Δ	$H(A\|UE) - I(V;A\|UW)$	$H(A\|UE) - I(V;A\|UW)$	$H(A\|UE) - I(V;A\|U)$

Table 2.1: The three corner points.

These schemes correspond to all possible combinations of the set $\{U, V, W\}$, provided that U is decoded prior to V, as summarized in row #2 of Table 2.1. For each scheme, the equivocation rate at Eve can be characterized following the argument of Section 2.3.6. After Fourier-Motzkin elimination [156] and classical manipulation, we can prove that the three proposed schemes achieve corner points (I), (II) and (III), which coordinates are given in Table 2.1.

Points (I) and (II) correspond to identical distortion and equivocation rate levels, say D and Δ (see Figure 2.4). By a time-sharing combination of these schemes, each point on segment (I)–(II) is also achievable and presents distortion D and equivocation rate Δ. This segment can be easily described since the quantity $R_A + R_C$ is identical for both points (I) and (II) (see Figure 2.3).

Points (II) and (III) correspond to identical distortion level, say D. By a time-sharing combination of these schemes, each point on segment (II)–(III) is also achievable and presents distortion D. This segment can be easily described since quantities $R_A + R_C$ and $\Delta - R_C$ are identical for both points (II) and (III) (see Figures 2.3 and 2.4, respectively).

Segments (I)–(II) and (II)–(III) define regions which union is delimited by six hyperplanes given by the equations of Theorem 2.1. □

Remark 2.3. Projections of points (I) and (III) on the plane $\Delta = 0$ i.e., when there is no secrecy constraint, are those obtained using Berger-Tung coding [9]. In this case, point (II) is useless since it is achievable by a time-sharing combination of points (I) and (III) (see Figure 2.3). In the general case, the proposed scheme can however improve the security of the transmission, as shown in Figure 2.4.

Remark 2.4. When there is no security requirement, Jana and Blahut [70] recently proved the equivalence of the inner bounds of [9] and [11], meaning that point (I) alone yields the same region that points (I) and (III) (after the convex hull operation). A similar result in our secure setting does not seem obvious.

Remark 2.5. The simple union of the regions given by the equations of Theorem 2.1 is not convex. In fact, a time-sharing variable T cannot be included in auxiliary variables U, V

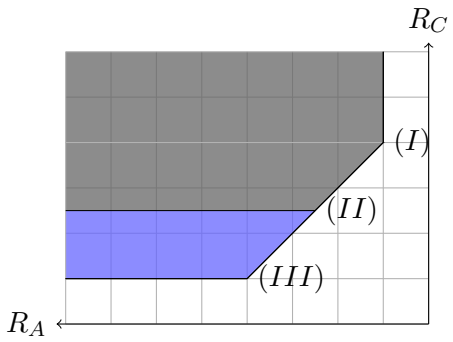


Figure 2.3: Projection on the plane $\Delta = 0$.

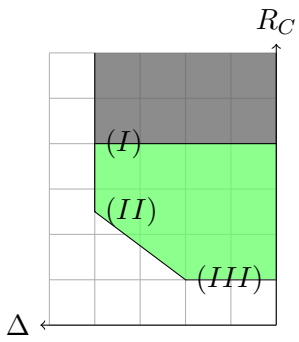


Figure 2.4: Projection on the plane $R_A = 0$.

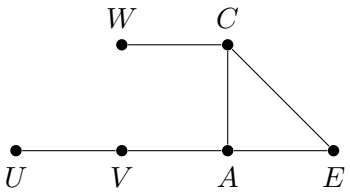


Figure 2.5: Inner bound–Graphical representation of probability distribution $p(uvwace)$.

and W. This would break the long Markov chain $U \multimap V \multimap A \multimap C \multimap W$ which is essential in our coding scheme (see also Figure 2.5, and Appendix B for details on such graphical representations).

The following proposition gives upper bounds on the cardinalities of alphabets $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$. The proof relies on Fenchel-Eggleston-Carathéodory's theorem and follows standard cardinality bounding argument (see [42, Appendix C]).

Proposition 2.2 (Cardinalities)**.** *In the single-letter characterization of region $\mathcal{R}_{in}$ given by Theorem 2.1, it suffices to consider sets $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$ such that $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 5$, $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 5)(\|\mathcal{A}\| + 3)$, and $\|\mathcal{W}\| \leq \|\mathcal{C}\| + 3$.*

Proof. See Appendix D.3. □

2.2.3 Outer bound

The following theorem gives an outer bound on region $\mathcal{R}^*$ i.e., it defines $\mathcal{R}_{\text{out}} \supseteq \mathcal{R}^*$.

Theorem 2.3 (Outer bound)**.** *Region $\mathcal{R}^*$ is included in $\mathcal{R}_{out}$, defined as the closure of the set of all tuples $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ such that there exist random variables U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, respectively, with joint distributions $p(wace) = p(w|c)p(ace)$, $p(uvace) = p(u|v)p(v|a)p(ace)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, verifying the following inequalities:*

$$\begin{aligned} R_A &\geq I(V;A|W)\,, \\ R_C &\geq I(W;C|V)\,, \\ R_A + R_C &\geq I(VW;AC)\,, \\ D &\geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\,, \\ \Delta &\leq H(A|VW) + I(A;W|U) - I(A;E|U)\,, \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V)\,. \end{aligned}$$

Proof. See Appendix D.4. □

As in the classical multiterminal source coding setup [9], the outer region resembles the inner region except that it is convex without time-sharing and that Markov chain conditions $W \multimap C \multimap (A,E)$ and $U \multimap V \multimap A \multimap (C,E)$ are weaker than the long Markov chain of Theorem 2.1 (compare Figures 2.5 and 2.6).

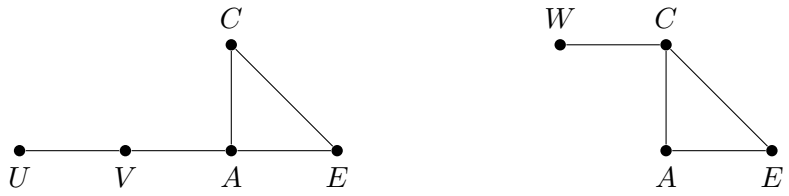


Figure 2.6: Outer bound–Graphical representation of probability distributions $p(uvace)$ and $p(wace)$.

2.2.4 Special case: Lossless reconstruction of A

In case of lossless reconstruction of A at Bob,[1] if Eve has no side information ($E = \emptyset$), then point (I) yields the optimal performance choosing auxiliary variables $U = \emptyset$ and $V = A$ i.e., using Wyner-Ahlswede-Körner coding [4, 163], as stated by Tandon et al. [147, Theorem 1]: In this case, region $\mathcal{R}^*$ writes as the closure of the set of all tuples $(R_A, R_C, D = 0, \Delta) \in \mathbb{R}_+^4$ such that there exists a random variable W on some finite set $\mathcal{W}$ s.t. $W \multimap C \multimap A$ form a Markov chain and

$$\begin{aligned} R_A &\geq H(A|W) \,, \\ R_C &\geq I(W;C) \,, \\ \Delta &\leq I(A;W) \,. \end{aligned}$$

2.2.5 Joint estimation and equivocation of both sources

Definition 2.2 only involves the distortion level at Bob and the equivocation rate at Eve about Alice's source. As a matter of fact, the proofs of Theorems 2.1 and 2.3 can be used to obtain inner and outer bounds on the achievable region when also considering a distortion constraint on Charlie's source at Bob. This requires the following additional inequality in the definition of the achievability:

$$\mathbb{E}\big[d_C\big(C^n, g_C(f_A(A^n), f_C(C^n))\big)\big] \leq D_C + \varepsilon \,,$$

for some distortion measure d_C and decoding function g_C. The resulting bounds will only differ from the ones of Theorems 2.1 and 2.3 by adding the following inequality:

$$D_C \geq \mathbb{E}\big[d_C(C, \hat{C}(V, W))\big] \,,$$

for some function $\hat{C} \colon \mathcal{V} \times \mathcal{W} \to \mathcal{C}$. For the sake of readability, we did not include this fifth dimension in the main definitions. In Section 2.5, we remove the distortion, addressing the case of lossless reconstruction of both sources, and prove that region $\mathcal{R}_{\text{in}}$ yields an optimal characterization of the corresponding achievable region.

[1] This case is included in the general setup choosing d as the Kronecker delta and $D = 0$.

Furthermore, the *joint* equivocation rate writes:

$$\frac{1}{n}H(A^nC^n|f_A(A^n),E^n) = \frac{1}{n}H(A^n|f_A(A^n),E^n) + \frac{1}{n}H(C^n|A^nE^n)\,.$$

The last term $\frac{1}{n}H(C^n|A^nE^n)$ is constant i.e., independent of the coding scheme. Hence, the results involving $\frac{1}{n}H(A^n|f_A(A^n),E^n)$ directly apply to the joint equivocation rate.

2.3 Proof of Theorem 2.1 (Inner bound)

Let U, V, W be three random variables on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, respectively, with joint distribution $p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace)$, a function $\hat{A}\colon \mathcal{V}\times\mathcal{W} \to \mathcal{A}$, and a tuple $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$. In this section, we describe a scheme that achieves (under some sufficient conditions) tuple (R_A, R_C, D, Δ) i.e., for any $\varepsilon > 0$, we construct an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) such that:

$$\mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] \leq D + \varepsilon\,,$$
$$\frac{1}{n}\,H(A^n|f_A(A^n),E^n) \geq \Delta - \varepsilon\,.$$

In this scheme, Alice (resp. Charlie) transmits to Bob a compressed version (U, V), with V on the top of U, (resp. W) of A (resp. C) using random binning. From the three bin indices, Bob *jointly* decodes variables U, V and W.

Let $\varepsilon > 0$, $R_1, R_2 \in \mathbb{R}_+^*$ such that $R_1 + R_2 = R_A + \varepsilon$, and $S_1 \geq R_1$, $S_2 \geq R_2$, $S_C \geq R_C + \varepsilon$. Define $\gamma = \frac{\varepsilon}{6\,d_{\max}}$.

2.3.1 Codebook generation

2.3.1.1 Alice's codebook

Randomly pick 2^{nS_1} sequences $u^n(s_1)$ from $T_\delta^n(U)$ and divide them into 2^{nR_1} equal size bins $B_1(r_1)$, $r_1 \in \{1, \ldots, 2^{nR_1}\}$. Then, for each codeword $u^n(s_1)$, randomly pick 2^{nS_2} sequences $v^n(s_1, s_2)$ from $T_\delta^n(V|u^n(s_1))$ and divide them into 2^{nR_2} equal size bins $B_2(s_1, r_2)$, $r_2 \in \{1, \ldots, 2^{nR_2}\}$. See Figure 2.7.

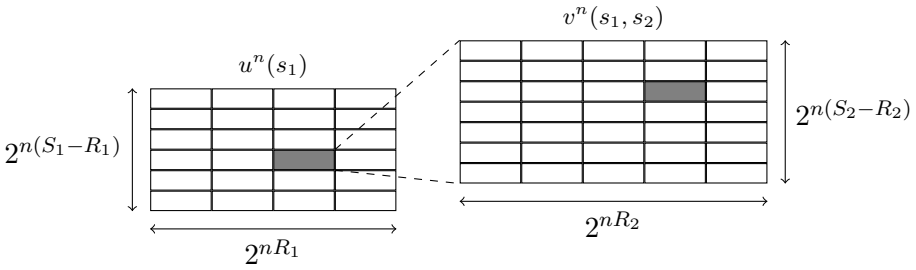


Figure 2.7: Alice's codebook.

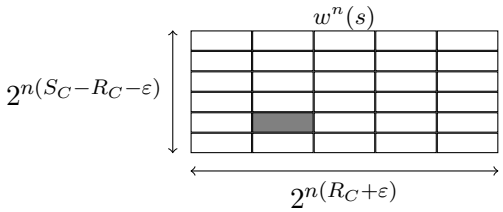


Figure 2.8: Charlie's codebook.

2.3.1.2 Charlie's codebook

Randomly pick 2^{nS_C} sequences $w^n(s)$ from $T_\delta^n(W)$ and divide them into $2^{n(R_C+\varepsilon)}$ equal size bins $B_C(r)$, $r \in \left\{1, \ldots, 2^{n(R_C+\varepsilon)}\right\}$. See Figure 2.8.

2.3.2 Encoding procedures

2.3.2.1 At Alice

Assume that sequence A^n is produced at Alice. Look for the first codeword $u^n(s_1)$ such that $(u^n(s_1), A^n) \in T_\delta^n(U, A)$. Then look for a codeword $v^n(s_1, s_2)$ such that $(v^n(s_1, s_2), A^n) \in T_\delta^n(V, A|u^n(s_1))$. Let $B_1(r_1)$ and $B_2(s_1, r_2)$ be the bins of $u^n(s_1)$ and $v^n(s_1, s_2)$, respectively. Alice sends the message $J = f_A(A^n) \triangleq (r_1, r_2)$ on her error-free link.

2.3.2.2 At Charlie

Assume that sequence C^n is produced at Charlie. Look for a codeword $w^n(s)$ such that $(w^n(s), C^n) \in T_\delta^n(W, C)$. Let $B_C(r)$ be the bin of $w^n(s)$. Charlie sends the message $K = f_C(C^n) \triangleq r$ on his error-free link.

2.3.3 Decoding procedure

Assume that Bob receives $J = (r_1, r_2)$ from Alice and $K = r$ from Charlie. Look for the unique *jointly typical* codewords (u^n, v^n, w^n) with bin indices (r_1, r_2, r) i.e., look for the unique indices (s_1, s_2, s) such that $(u^n(s_1), v^n(s_1, s_2), w^n(s)) \in (B_1(r_1) \times B_2(s_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W)$. Then compute the estimate $g(J, K) \in \mathcal{A}^n$ using the following component-wise relation, for each $i = \{1, \ldots, n\}$:

$$g_i(J, K) \triangleq \hat{A}(v_i(s_1, s_2), w_i(s)) \, .$$

2.3.4 Errors and constraints

Denoting by E the event "An error occurred during the encoding or decoding steps," we expand its probability (averaged over the set of all possible codebooks) as follows: $\Pr\{\mathsf{E}\} \leq P_t + P_{e,1} + P_{e,2} + P_{e,3} + P_d$, where each term corresponds to a particular error

event, as detailed below. We derive sufficient conditions on the parameters that make each of these probabilities small.

2.3.4.1 Typicality

From standard properties of typical sequences (see Appendix A), there exists a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that $P_t \triangleq \Pr\{(A^n, C^n, E^n) \notin T_\delta^n(A, C, E)\} \leq \eta_n$. Consequently, $P_t \leq \gamma$ for some sufficiently large n.

2.3.4.2 Encoding at Alice

In the first encoding step, Alice needs to find (at least) one codeword $u^n(s_1)$ such that $(u^n(s_1), A^n) \in T_\delta^n(U, A)$. The corresponding error probability $P_{e,1}$ writes:

$$\begin{aligned}
P_{e,1} &\triangleq \Pr\{\nexists\, s_1 : (u^n(s_1), A^n) \in T_\delta^n(U, A)\} \\
&= \left(\Pr\left\{(U^n, A^n) \notin T_\delta^n(U, A) \;\middle|\; U^n \in T_\delta^n(U), A^n \in T_\delta^n(A)\right\}\right)^{2^{nS_1}} \\
&= \left(1 - \Pr\left\{(U^n, A^n) \in T_\delta^n(U, A) \;\middle|\; U^n \in T_\delta^n(U), A^n \in T_\delta^n(A)\right\}\right)^{2^{nS_1}} \\
&\leq 2^{-2^{nS_1} \Pr\left\{(U^n, A^n) \in T_\delta^n(U, A) \;\middle|\; U^n \in T_\delta^n(U), A^n \in T_\delta^n(A)\right\}} \\
&\leq 2^{-2^{nS_1} 2^{-n(I(U;A)+\eta_n)}},
\end{aligned}$$

for some sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ (see Lemma A.4 in Appendix A). If $S_1 > I(U; A)$, then probability $P_{e,1}$ vanishes as n tends to infinity, and hence can be upper bounded by γ for some sufficiently large n.

Similarly, the second encoding step succeeds with probability $1 - P_{e,2} \geq 1 - \gamma$ under condition $S_2 > I(V; A|U)$.

2.3.4.3 Encoding at Charlie

In his encoding step, Charlie needs to find (at least) one codeword $w^n(s)$ such that $(w^n(s), C^n) \in T_\delta^n(W, C)$. Following the above argument, the corresponding error probability $P_{e,3}$ can be upper bounded by γ under condition $S_C > I(W; C)$.

2.3.4.4 Decoding

The decoding error probability P_d must be carefully handled. An error occurs when the decoded tuple differs from the original one (s_1, s_2, s). There are three meaningful possible

events so that P_d writes:[2]

$$\begin{aligned} P_d &\triangleq \Pr\{\cancel{(s_1, s_2, s)}\} \\ &= \Pr\{\{\cancel{s}\} \cup \{\cancel{s_1}, \check{s}\} \cup \{\check{s}_1, \cancel{s_2}, \check{s}\}\} \\ &\leq \Pr\{\cancel{s}\} + \Pr\{\cancel{s_1}, \check{s}\} + \Pr\{\check{s}_1, \cancel{s_2}, \check{s}\} \ . \end{aligned} \tag{2.7}$$

From classical arguments, we can prove the following lemma, which gives sufficient conditions that make each term of the r.h.s. of (2.7) small.

Lemma 2.4. *The following holds true:*

$$S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V;W) \implies \Pr\{\cancel{s}\} \xrightarrow[n\to\infty]{} 0 \ , \tag{2.8}$$

$$S_1 - R_1 + S_2 - R_2 < I(V;W) \implies \Pr\{\cancel{s_1}, \check{s}\} \xrightarrow[n\to\infty]{} 0 \ , \tag{2.9}$$

$$S_2 - R_2 < I(V;W|U) \implies \Pr\{\check{s}_1, \cancel{s_2}, \check{s}\} \xrightarrow[n\to\infty]{} 0 \ . \tag{2.10}$$

Proof. See Appendix D.1. □

If the conditions given by Lemma 2.4 are verified, then $P_d \leq \gamma$ for some sufficiently large n.

2.3.4.5 Summary

In this paragraph, we proved that under some sufficient conditions, $\Pr\{\mathsf{E}\} \leq 5\gamma$.

2.3.5 Distortion at Bob

We now check that our code achieves the required distortion level at Bob (averaged over the set of all possible codebooks):

$$\begin{aligned} &\mathbb{E}\Big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\Big] \\ &\qquad \leq (1 - \Pr\{\mathsf{E}\})\mathbb{E}\left[d\big(A^n, \hat{A}\big(v^n(s_1,s_2), w^n(s)\big)\big)\middle|\cancel{\mathsf{E}}\right] + \Pr\{\mathsf{E}\}\, d_{\max} \\ &\qquad \leq \mathbb{E}\big[d(A, \hat{A}(V,W))\big] + \frac{\varepsilon}{6} + \frac{5\varepsilon}{6} \ , \end{aligned} \tag{2.11}$$

where the last inequality holds for some sufficiently large n, and follows from $\Pr\{\mathsf{E}\} \leq 5\gamma$, the definition of γ, and the argument below.

[2] We denote by $\check{s}$ the event "Index s has been correctly decoded", and $\cancel{s}$ its complement. Same notation holds for indices s_1, s_2, and any tuple of indices.

For each $(a^n, v^n, w^n) \in T_\delta^n(A, V, W)$,

$$\begin{aligned} d\big(a^n, \hat{A}\big(v^n, w^n\big)\big) &= \frac{1}{n}\sum_{i=1}^{n} d\big(a_i, \hat{A}\big(v_i, w_i\big)\big) \\ &= \frac{1}{n}\sum_{(a,v,w)\in\mathcal{A}\times\mathcal{V}\times\mathcal{W}} d\big(a, \hat{A}(v,w)\big) N(a,v,w|a^n, v^n, w^n) \\ &= \mathbb{E}\big[d(A, \hat{A}(V,W))\big] \\ &\quad + \sum_{(a,v,w)\in\mathcal{A}\times\mathcal{V}\times\mathcal{W}} d\big(a, \hat{A}(v,w)\big)\left(\frac{1}{n}N(a,v,w|a^n, v^n, w^n) - p(a,v,w)\right) \\ &\leq \mathbb{E}\big[d(A, \hat{A}(V,W))\big] + d_{\max}\,\|\mathcal{A}\|\,\|\mathcal{V}\|\,\|\mathcal{W}\|\,\delta_n\,, \end{aligned}$$

where the last inequality follows from the definition of typical sequences (see Appendix A). Inequality (2.11) then follows from the fact that $(A^n, v^n(s_1, s_2), w^n(s)) \in T_\delta^n(A, V, W)$ when no error occurred, and $\delta_n \xrightarrow[n\to\infty]{} 0$ (see the Delta-Convention in Appendix A).

Condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V,W))\big]$ is thus sufficient to achieve distortion $D + \varepsilon$ at Bob.

2.3.6 Equivocation rate at Eve

The equivocation rate at Eve (averaged over the set of all possible codebooks) can be lower bounded as follows:

$$\begin{aligned} \frac{1}{n}H(A^n|f_A(A^n), E^n) &= \frac{1}{n}H(A^n|r_1 r_2 E^n) \\ &= \frac{1}{n}\Big[H(A^n|r_1 E^n) - I(A^n; r_2|r_1 E^n)\Big] \\ &\overset{(a)}{\geq} \frac{1}{n}\Big[H(A^n|s_1 E^n) - H(r_2)\Big] \\ &\overset{(b)}{\geq} H(A|UE) - R_2 - \varepsilon\,, \end{aligned} \tag{2.12}$$

where

- step (a) follows from the facts that the bin index r_1 is a deterministic function of the codeword index s_1, the bin index r_2 is a deterministic function of A^n, and conditioning reduces the entropy,
- step (b) for some sufficiently large n, from Lemma 2.5 below, and $r_2 \in \{1, \ldots, 2^{nR_2}\}$.

From the encoding procedure described in Section 2.3.2.1 and standard properties of typical sequences, we can prove the following lemma.

Lemma 2.5. *The following inequality holds for some sequence $\eta_n \xrightarrow[n\to\infty]{} 0$:*

$$H(A^n|s_1 E^n) \geq n(H(A|UE) - \eta_n)\,.$$

Proof. See Appendix D.2. □

Inequality (2.12) indicates that condition $\Delta \leq H(A|UE) - R_2$ is sufficient to achieve equivocation rate $\Delta - \varepsilon$.

2.3.7 End of proof

In this section, we proved that sufficient conditions for the achievability of a tuple (R_A, R_C, D, Δ) are given by the following system of inequalities, for each $\varepsilon > 0$:

$$\begin{cases} R_1 > 0 \\ R_2 > 0 \\ R_A + \varepsilon = R_1 + R_2 \\ R_C \geq 0 \\ S_1 \geq R_1 \\ S_2 \geq R_2 \\ S_C \geq R_C + \varepsilon \\ S_1 > I(U;A) \\ S_2 > I(V;A|U) \\ S_C > I(W;C) \\ S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V;W) \\ S_1 - R_1 + S_2 - R_2 < I(V,W) \\ S_2 - R_2 < I(V;W|U) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V,W))\big] \\ \Delta \leq H(A|UE) - R_2 \end{cases}$$

Fourier-Motzkin elimination [156] then yields:

$$\begin{cases} R_A + \varepsilon > I(V;A|W) \\ R_C + \varepsilon > I(W;C|V) \\ R_A + R_C + 2\varepsilon > I(VW;AC) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V,W))\big] \\ \Delta < H(A|VW) + I(A;W|U) - I(A;E|U) \\ \Delta - R_C - \varepsilon < H(A|V) - I(A;E|U) - I(W;C|V) \end{cases}$$

This proves Theorem 2.1. □

2.4 Secure lossy source coding with uncoded side information

In this section, we consider the special case depicted in Figure 2.9 where Bob has access to *uncoded* side information i.e., Bob and Charlie are collocated.

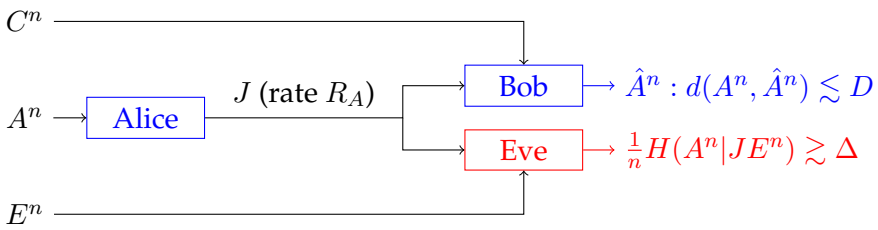


Figure 2.9: Secure lossy source coding with uncoded side information.

2.4.1 Definitions

We need the following new definitions.

Definition 2.3 (Code). An (n, R_A)-code for source coding in this setup is defined by

- an encoding function at Alice $f\colon \mathcal{A}^n \to \{1, \dots, 2^{nR_A}\}$,
- a decoding function at Bob $g\colon \{1, \dots, 2^{nR_A}\} \times \mathcal{C}^n \to \mathcal{A}^n$.

Definition 2.4 (Achievability). A tuple $(R_A, D, \Delta) \in \mathbb{R}_+^3$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an $(n, R_A + \varepsilon)$-code (f, g) such that:

$$\mathbb{E}\left[d\big(A^n, g(f(A^n), C^n)\big)\right] \leq D + \varepsilon\,,$$
$$\frac{1}{n} H(A^n|f(A^n), E^n) \geq \Delta - \varepsilon\,.$$

The set of all such achievable tuples is denoted by $\mathcal{R}^*_{\text{uncoded}}$ and is referred to as the *rate-distortion-equivocation region*.

2.4.2 Optimal characterization

The following theorem provides a single-letter characterization of region $\mathcal{R}^*_{\text{uncoded}}$.

Theorem 2.6 (Single-letter characterization). *Region $\mathcal{R}^*_{uncoded}$ writes as the closure of the set of all tuples $(R_A, D, \Delta) \in \mathbb{R}_+^3$ such that there exist random variables U, V on some finite sets $\mathcal{U}$, $\mathcal{V}$, resp., with joint distribution $p(uvace) = p(u|v)p(v|a)p(ace)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, verifying the following inequalities:*

$$R_A \geq I(V; A|C)\,, \tag{2.13}$$
$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, C))\big]\,, \tag{2.14}$$
$$\Delta \leq H(A|VC) + I(A; C|U) - I(A; E|U)\,. \tag{2.15}$$

Proof. The achievability follows from the one of Theorem 2.1, choosing auxiliary variable $W = C$, and removing the constraints on R_C (letting R_C tend to ∞) i.e., from the achievability of point (I) (see Figure 2.10).

A new proof is needed for the converse part (see Appendix D.5). □

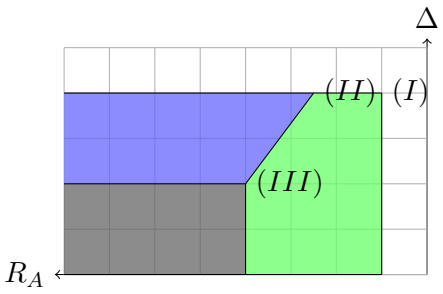


Figure 2.10: Projection on the plane $R_C = 0$.

Comments similar to the ones of Section 2.2.2 about Theorem 2.1 are also relevant here: (2.13) and (2.14) are classical in rate-distortion theory; Alice can exploit the admissible distortion at Bob to increase the equivocation rate at Eve (see term $H(A|VC)$ in (2.15)); and auxiliary variable U can be tuned to maximize $I(A;C|U) - I(A;E|U)$.

Remark 2.6. If Eve is a legitimate decoder that wishes to estimate the source A within a certain distortion criterion (instead of an eavesdropper that other terminals must contend with), then [152] provides inner and outer bounds on the corresponding rate-distortion function (with two decoders and side-informations). Finding an optimal characterization of the achievable region in such a case is still an open problem.

The following proposition gives upper bounds on the cardinalities of alphabets $\mathcal{U}$, $\mathcal{V}$.

Proposition 2.7 (Cardinalities). *In the single-letter characterization of region $\mathcal{R}^*_{uncoded}$ given by Theorem 2.6, it suffices to consider sets $\mathcal{U}$ and $\mathcal{V}$ such that $\|\mathcal{U}\| \leq \|\mathcal{A}\| + 2$, and $\|\mathcal{V}\| \leq (\|\mathcal{A}\| + 2)(\|\mathcal{A}\| + 1)$.*

Proof. The proof is similar to the one of Proposition 2.2 (given in Appendix D.3). Details are omitted. □

2.4.3 Alternative characterization

The following proposition can be easily proved from Theorem 2.6.

Proposition 2.8 (Alternative characterization). *Region $\mathcal{R}^*_{uncoded}$ writes as the closure of the set of all tuples $(R_A, D, \Delta) \in \mathbb{R}^3_+$ such that there exist random variables U, V on some finite sets $\mathcal{U}$, $\mathcal{V}$, respectively, with joint distribution $p(uvace) = p(u|v)p(v|a)p(ace)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, verifying the following inequalities:*

$$R_A \geq \Big[I(U;C) - I(U;E)\Big]_+ + I(V;A|C)\,, \tag{2.16}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\,, \tag{2.17}$$

$$\Delta \leq H(A|VC) + I(A;C|U) - I(A;E|U)\,. \tag{2.18}$$

Proof. Inequalities (2.16)–(2.18) yield a smaller region than (2.13)–(2.15). The achievability of the above proposition thus follows from the one of Theorem 2.6.

Notice that the r.h.s. of (2.15) and (2.18) writes

$$H(A|VC) + I(A;C) - I(A;E) - \Big[I(U;C) - I(U;E)\Big] .$$

Maximizing this term w.r.t. U thus boils down to minimizing $I(U;C) - I(U;E)$. In the worst case, setting $U = \emptyset$ makes this term zero, meaning that the optimal choice U^* always leads to $I(U^*;C) - I(U^*;E) \leq 0$, and makes (2.13) and (2.16) identical. □

Proposition 2.8, along with the above proof, indicates that the optimal choice of U is a random variable U^* that can be decoded by Eve. Since minimizing quantity $I(U;C) - I(U;E)$ w.r.t. U corresponds to looking for a part of V which conveys more information about E than C, this *common message* should however give little information to Eve.

2.4.4 Special cases of interest

2.4.4.1 Lossless secure source coding

In case of lossless reconstruction of A at Bob, the following corollary directly follows from Theorem 2.6.

Corollary 2.9. *In case of lossless reconstruction of A at Bob, region $\mathcal{R}^*_{uncoded}$ reduces to the closure of the set of all tuples $(R_A, D = 0, \Delta) \in \mathbb{R}^3_+$ such that there exists a random variable U on some finite set $\mathcal{U}$, such that $U \multimap A \multimap (C, E)$ form a Markov chain and*

$$\begin{aligned} R_A &\geq H(A|C) , \\ \Delta &\leq I(A;C|U) - I(A;E|U) . \end{aligned}$$

Remark 2.7. In case of a noiseless public link of unlimited capacity i.e., $R_A \to \infty$, the authors of [131] studied the so-called *leakage rate*, defined as $\liminf \frac{1}{n} I(A^n; JE^n)$, which equals $H(A) - \Delta$. Their result "When Bob remains silent" [131, Theorem 1] thus follows as a special case of Corollary 2.9.

2.4.4.2 Bob has less noisy side information than Eve ($C \succeq_A E$)

Corollary 2.10. *If Bob has less noisy side information than Eve, then region $\mathcal{R}^*_{uncoded}$ reduces to the closure of the set of all tuples $(R_A, D, \Delta) \in \mathbb{R}^3_+$ such that there exist a random variable V on some finite set $\mathcal{V}$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$ such that $V \multimap A \multimap (C, E)$ form a Markov chain and*

$$\begin{aligned} R_A &\geq I(V;A|C) , \\ D &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big] , \\ \Delta &\leq H(A|VC) + I(A;C) - I(A;E) . \end{aligned}$$

In this case, random variable U of Theorem 2.6 is set to a constant value, and hence Wyner-Ziv coding [166] achieves the whole region.

2.4.4.3 Eve has less noisy side information than Bob ($E \succeq_A C$)

Corollary 2.11. *If Eve has less noisy side information than Bob, then region $\mathcal{R}^*_{uncoded}$ reduces to the closure of the set of all tuples $(R_A, D, \Delta) \in \mathbb{R}^3_+$ such that there exist a random variable V on some finite set $\mathcal{V}$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$ such that $V \multimap A \multimap (C, E)$ form a Markov chain and*

$$\begin{aligned} R_A &\geq I(V;A|C)\ , \\ D &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\ , \\ \Delta &\leq H(A|VE)\ . \end{aligned}$$

In this case, random variable U of Theorem 2.6 is set to V, and hence Wyner-Ziv coding [166] achieves the whole region. The equivocation rate at Eve corresponds to the case where Eve can reliably decode V. Here, Alice can only exploit the available distortion at Bob to achieve a non-zero equivocation rate at Eve.

2.5 Secure distributed lossless compression

2.5.1 Definitions

In this section, we consider the case where Bob wants to perfectly reconstruct both sources A and C, from messages J and K i.e., *distributed lossless compression*, as depicted in Figure 2.11. We need the following new definitions:

Definition 2.5 (Code)**.** An (n, R_A, R_C)-code for distributed compression in this setup is defined by

- an encoding function at Alice $f_A\colon \mathcal{A}^n \to \{1, \dots, 2^{nR_A}\}$,
- an encoding function at Charlie $f_C\colon \mathcal{C}^n \to \{1, \dots, 2^{nR_C}\}$,
- a decoding function at Bob $g\colon \{1, \dots, 2^{nR_A}\} \times \{1, \dots, 2^{nR_C}\} \to \mathcal{A}^n \times \mathcal{C}^n$.

Definition 2.6 (Achievability)**.** A tuple $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) such that:

$$\begin{aligned} \Pr\left\{g(f_A(A^n), f_C(C^n)) \neq (A^n, C^n)\right\} &\leq \varepsilon\ , \\ \frac{1}{n} H(A^n|f_A(A^n), E^n) &\geq \Delta - \varepsilon\ . \end{aligned}$$

The set of all such achievable tuples is denoted by $\mathcal{R}^*_{\text{lossless}}$ and is referred to as the *compression-equivocation rates region*.

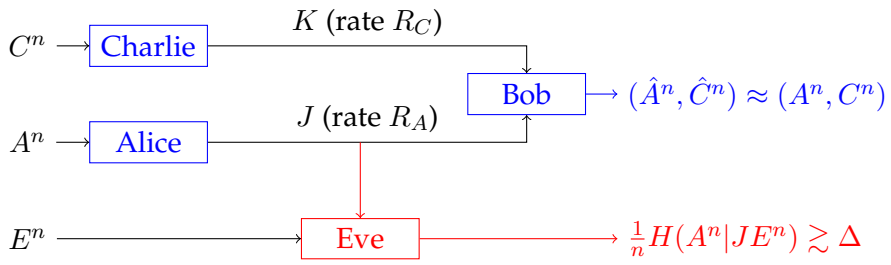


Figure 2.11: Secure distributed lossless compression.

2.5.2 Optimal characterization

The following theorem provides a single-letter characterization of region $\mathcal{R}^*_{\text{lossless}}$.

Theorem 2.12 (Single-letter characterization)**.** *Region $\mathcal{R}^*_{lossless}$ writes as the closure of the set of all tuples $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ such that there exists a random variable U on some finite set $\mathcal{U}$ verifying the Markov chain $U \multimap A \multimap (C, E)$, and the following inequalities:*

$$R_A \geq H(A|C) \,, \tag{2.19}$$

$$R_C \geq H(C|U) \,, \tag{2.20}$$

$$R_A + R_C \geq H(AC) \,, \tag{2.21}$$

$$\Delta \leq I(A; C|U) - I(A; E|U) \,. \tag{2.22}$$

Proof. The achievability follows from the one of points (I) and (II), choosing auxiliary variables $V = A$ and $W = C$ (see Section 2.2.2).

A new proof is needed for the converse part (see Appendix D.6). □

Inequalities (2.19)–(2.21) resemble the ones of Slepian and Wolf [143, Section III]. They ensure perfect reconstruction of both variables A and C at Bob. Depending on the distribution of (A, C, E), variable U can be tuned to allow non-zero equivocation rate at Eve (see (2.22)). If the side information at Eve E is *less noisy* than C i.e., $E \succeq_A C$, then setting $U = A$ is optimal, and hence Slepian-Wolf coding achieves the whole region (with $\Delta = 0$).

In case of uncoded side information at Bob, Theorem 2.12 directly yields Corollary 2.9 letting R_C tend to infinity.

Remark 2.8. As a matter of fact, the above result refines recent ones [55, 95] which only provide inner and outer bounds on $\mathcal{R}^*_{\text{lossless}}$. It should be mentioned here that the outer bound of [95, Chapter 8], [55, 56] is incorrect. We use [55] as the main reference, but comments below also apply to [95, Chapter 8] and [56] as well. [55, Eq. (5)] writes $\Delta \geq [H(A|E) - R_A]_+$, meaning that points with $\Delta = 0$ are not always included in the considered region, while zero equivocation rate is achievable by any coding scheme. This inequality can thus not be proved in the converse part. In fact, [55, Eq. (29)] is derived using $H(A^N|E^N, J) \leq \Delta$, while only the reverse inequality holds.

2.5.3 Alternative characterization

As in Section 2.4 for lossy source coding with uncoded side information, we can also provide here an alternative characterization of region $\mathcal{R}^*_{\text{lossless}}$.

Proposition 2.13 (Alternative characterization). *Region $\mathcal{R}^*_{lossless}$ writes as the closure of the set of all tuples $(R_A, R_C, \Delta) \in \mathbb{R}^3_+$ such that there exists a random variable U on some finite set $\mathcal{U}$ verifying the Markov chain $U \multimap A \multimap (C, E)$, and the following inequalities:*

$$R_A \geq \big[I(U;C) - I(U;E)\big]_+ + H(A|C)\,, \tag{2.23}$$

$$R_C \geq H(C|U)\,, \tag{2.24}$$

$$R_A + R_C \geq H(AC)\,, \tag{2.25}$$

$$\Delta \leq I(A;C|U) - I(A;E|U)\,. \tag{2.26}$$

Proof. The achievability follows from the one of Theorem 2.12.

A new proof is needed for the converse part (see Appendix D.7). □

This new single-letter characterization means that *giving U to Eve is also optimal*. The corresponding additional rate $[I(U;C) - I(U;E)]_+$ does not lead to a lower equivocation at Eve. This should be considered with reference to known results on the wiretap channel [32,90], where the so called *common message* can be chosen so that Eve also decodes it, without changing the achievable region.

2.6 Application examples

2.6.1 Gaussian sources with coded side information

Consider the source model depicted in Figure 2.12 where the source at Alice is standard Gaussian, and observations at Charlie and Eve are the outputs of independent additive white Gaussian noise (AWGN) channels with input A, gains ρ_C, ρ_E, and noise powers $(1-\rho_C^2)$, $(1-\rho_E^2)$, resp., for some $0 < \rho_C, \rho_E < 1$.

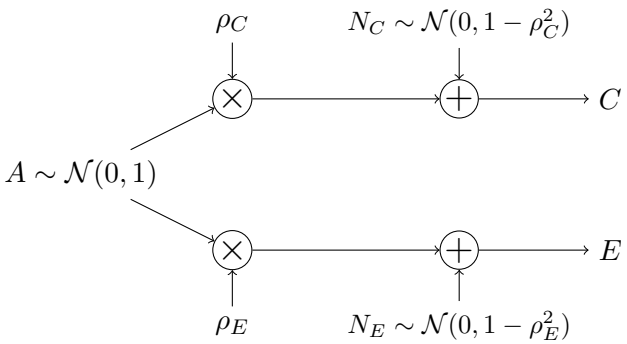


Figure 2.12: A model for Gaussian sources.

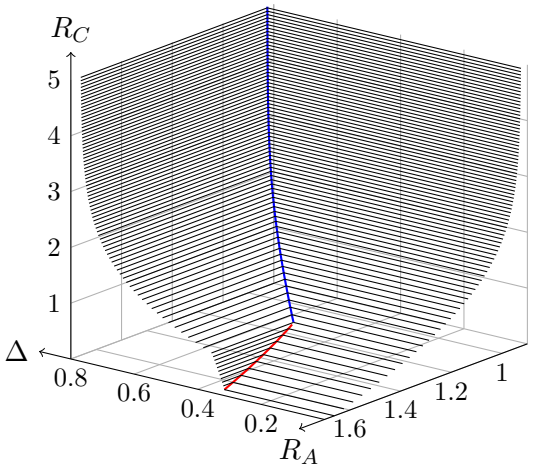


Figure 2.13: Achievable tuples in the Gaussian case ($\rho_C = 0.8$, $\rho_E = 0.6$, $D = 0.1$).

Although Theorem 2.1 is stated and proved for finite alphabet sources, we take the liberty to use its statement, with the appropriate quadratic distortion measure i.e., the Euclidean distance on $\mathbb{R}$ ($d(a,b) = (a-b)^2$, for each $a, b \in \mathbb{R}$), as an achievable region also for Gaussian sources (using differential entropy $h(\cdot)$, and considering any equivocation rates $\Delta \in \mathbb{R}$). In this setup, the *rates-distortion-equivocation region* is denoted by $\mathcal{R}^*_{\text{Gaussian}}$. Notice that the results should be generalizable to more general continuous-alphabet sources.

Remark 2.9. In this Gaussian setup, an achievable equivocation rate Δ provides a lower bound $2^{2\Delta}/(2\pi e)$ on the minimum mean-square error of any estimator of A at Eve (see e.g. [31, Theorem 8.6.6]).

Proposition 2.14 below provides an inner bound on $\mathcal{R}^*_{\text{Gaussian}}$ based on the achievability of point (I) (see Section 2.2.2) with Gaussian auxiliary variables. This choice is motivated by [119, Theorem 1] where Oohama proved that it is optimal when only one source is to be estimated within a certain distortion level (with no security constraint). Figure 2.13 shows a numerical evaluation of this region for $\rho_C = 0.8$, $\rho_E = 0.6$, $D = 0.1$.

Proposition 2.14 (Inner bound). *A tuple* $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$ *is achievable if:*

$$
\begin{aligned}
R_A &\geq \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+, \\
\Delta &\leq \frac{1}{2}\log\left(2\pi e(1-\rho_E^2)\right) \\
&\qquad -\frac{1}{2}\min\left\{\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+; \right. \\
&\qquad\qquad \left. \log\left(1+(1-\rho_E^2)\left[\frac{1}{D}-\frac{1}{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}\right]_+\right)\right\}.
\end{aligned}
$$

Proof. See Appendix D.8. □

If Eve has no side information i.e., $\rho_E = 0$, then the inner bound given by Proposition 2.14, and corresponding to Oohama coding [119], is optimal.

Proposition 2.15 (Optimal characterization). *If $\rho_E = 0$, then region $\mathcal{R}^*_{Gaussian}$ reduces to the set of all tuples $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^2 \times \mathbb{R}_+^* \times \mathbb{R}$ verifying the following inequalities:*

$$R_A \geq \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+,$$
$$\Delta \leq \frac{1}{2}\log(2\pi e) - \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+.$$

Proof. The achievability comes from Proposition 2.14.

The proof of the converse part follows the argument of [119] (see Appendix D.9). □

Remark 2.10. In case of *uncoded* side information at Bob i.e., $R_C \to \infty$, the inner bound provided by Proposition 2.14 is optimal if $\rho_C \geq \rho_E$ i.e., $C \succeq_A E$. We conjecture that it also holds if $\rho_C < \rho_E$, while the proof seems more tricky.

2.6.2 Binary source with (uncoded) BEC/BSC side informations

Consider the source model depicted in Figure 2.14, where the source is binary uniformly distributed and the side information at Bob, resp. Eve, is the output of a binary erasure channel (BEC) with erasure probability $\beta \in [0,1]$, resp. a binary symmetric channel (BSC) with crossover probability $\epsilon \in [0, \frac{1}{2}]$, with input A. The Hamming distance is used as distortion measure at Bob d.

This model is of interest since neither Bob nor Eve can always be a less-noisy decoder for all values of (β, ϵ). According to the values of the parameters (β, ϵ), it can be shown by means of standard manipulations [113] that the broadcast channel with input A and outputs (C, E) satisfies the following properties:

(*a*) If $0 \leq \beta \leq 2\epsilon$, E is a stochastically degraded version of C;

(*b*) If $2\epsilon \leq \beta \leq 4\epsilon(1-\epsilon)$, C is less noisy than E i.e., $C \succeq_A E$;

(*c*) If $4\epsilon(1-\epsilon) \leq \beta \leq h_2(\epsilon)$, C is more capable than E i.e., $I(A;C) \geq I(A;E)$;

(*d*) If $h_2(\epsilon) < \beta \leq 1$, none of the above relations hold between C and E.

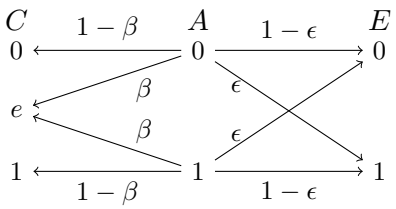


Figure 2.14: Binary source with BEC/BSC side informations.

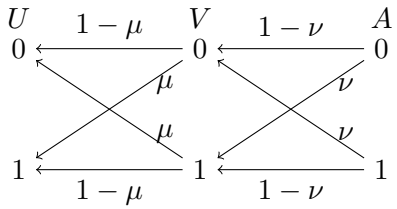


Figure 2.15: Binary auxiliary random variables.

Corollary 2.10 thus provides an optimal characterization of region $\mathcal{R}^*_{\text{uncoded}}$ when β lies in region (*a*) or (*b*). Otherwise, only Theorem 2.6 applies for the general case and variable U is neither constant nor equal to V.

We know from the cardinality constraints given in Proposition 2.7 that it suffices to consider sets $\mathcal{U}$ and $\mathcal{V}$ such that $\|\mathcal{U}\| \leq 4$ and $\|\mathcal{V}\| \leq 12$. As a matter of fact, according to the following proposition, we can restrict our attention to the auxiliary variables (U, V) obtained as the outputs of a degraded binary symmetric broadcast channel with input A, as depicted in Figure 2.15. Notice that V is identical to the auxiliary variable used by Wyner and Ziv [166] for the rate-distortion function of a binary source in the case where there is no eavesdropper.

Proposition 2.16 (Optimal characterization)**.** *Region $\mathcal{R}^*_{uncoded}$ writes as the set of all tuples $(R_A, D, \Delta) \in \mathbb{R}^3_+$ such that there exist $\nu, \mu \in [0, \frac{1}{2}]$ satisfying the following inequalities:*

$$\begin{aligned} R_A &\geq \beta\,(1 - h_2(\nu))\,, \\ D &\geq \beta\,\nu\,, \\ \Delta &\leq \beta\,h_2(\nu) + (1-\beta)\,h_2(\nu \star \mu) - h_2(\epsilon \star \nu \star \mu) + h_2(\epsilon)\,. \end{aligned}$$

Proof. The achievability part is a direct application of Theorem 2.6: define auxiliary random variables U and V as depicted in Figure 2.15, and function $\hat{A}$ on $\mathcal{V} \times \mathcal{C} = \{0,1\} \times \{0, e, 1\}$ by

$$\hat{A}(v,c) = \begin{cases} c & \text{if } c \neq e \\ v & \text{otherwise} \end{cases}$$

Expressions of Proposition 2.16 follow after some straightforward derivations.

The proof of the converse part is given in Appendix D.10. □

Remark 2.11. In this binary case with Hamming distance as distortion measure, an achievable distortion level D is an upper bound on the average bit error rate (BER) at Bob (while estimating A):

$$\mathbb{E}\big[d(A^n, g(f(A^n), C^n))\big] = \frac{1}{n}\sum_{i=1}^{n} \Pr\left\{\hat{A}_i \neq A_i\right\}\,,$$

where $\hat{A}_i \triangleq g_i(f_A(A^n), C^n)$ is the i-th coordinate of the estimate of A^n at Bob. At the same time, an achievable equivocation rate Δ provides a lower bound $h_2^{-1}(\Delta)$ on the

BER at Eve, as shown by the following inequality which holds for any $\breve{A}^n \in \mathcal{A}^n$ such that $\breve{A}^n \multimap (J, E^n) \multimap A^n$ form a Markov chain:

$$\frac{1}{n} H(A^n|JE^n) \leq h_2\left(\frac{1}{n}\sum_{i=1}^{n} \Pr\left\{\breve{A}_i \neq A_i\right\}\right) .$$

The proof relies on the fact that function h_2 is concave together with Jensen's inequality.

Numerical results

Using the inequalities of Proposition 2.16, we now numerically compute some achievable tuples for $\epsilon = 0.1$ and $\beta = h_2(\epsilon) \approx 0.469$ (see Figure 2.16). In case of lossless compression (columns #1 and #2 of Table 2.2), the auxiliary random variable V is set to A i.e., $\nu = 0$. Variable U actually enables a non-zero equivocation level. Now assume that the coding rate is limited to a maximum of 80% of the required rate for perfect reconstruction of the source (column #3). This induces a distortion of 0.015 at Bob and an equivocation rate of 0.133 bits at Eve. Even a small increase in the distortion at Bob can be fully exploited by Alice to achieve very significant gains (more than third times in this case) in terms of equivocation rate at Eve. Moreover, for distortion levels higher than 0.036, Wyner-Ziv coding actually achieves the optimal performance, as shown in Figure 2.16.

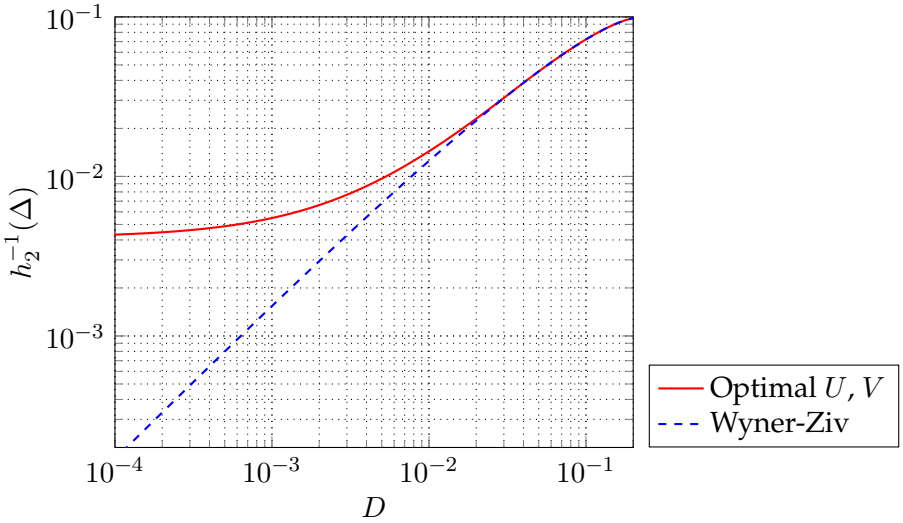


Figure 2.16: Uncertainty at Eve $h_2^{-1}(\Delta)$ as a function of the distortion level at Bob D ($\epsilon = 0.1$, $\beta = h_2(\epsilon) \approx 0.469$).

	Optimal	Slepian-Wolf	Optimal	Wyner-Ziv
Rate R	0.469	0.469	0.375	0.375
Distortion D	0	0	0.015	0.015
Equivocation rate Δ	0.039	0	0.133	0.126
ν	0	0	0.031	0.031
μ	0.078	0	0.050	0

Table 2.2: Some achievable tuples and corresponding parameters for auxiliary random variables ($\epsilon = 0.1$, $\beta = h_2(\epsilon) \approx 0.469$).

2.7 Summary

In this chapter, we have addressed the general problem of secure lossy source coding with coded side information. Inner and outer bounds on the corresponding achievable region have been derived. This setting can be seen as the natural extension of the Berger et al. problem [11] by taking the security requirements into account. It should be mentioned here that the latter is a fundamental information-theoretic problem for which the best known inner bound is not optimal in general. In the same way, our proposed bounds do not match in general, but the achievable inner region turns out to be optimal for two cases of particular interest. Namely, secure lossy source coding with uncoded side information, and secure distributed lossless compression. Interestingly enough, it is proved for both cases that there is no loss in coding to provide a *common* description of the source to both receivers, the legitimate one and the eavesdropper. The remaining information is intended to the legitimate receiver and considered at the eavesdropper as "raw" bits. Furthermore, under certain conditions (e.g., *less noisy*), the standalone Wyner-Ziv (or Slepian-Wolf) coding scheme can achieve the entire region and hence the highest security is guaranteed without additional efforts.

Application examples to secure lossy source coding of Gaussian and binary sources have been considered. The binary model is of interest since neither Bob nor Eve can always be a less-noisy decoder and thus the encoding strategy needed to achieve the whole region is rather novel. In the Gaussian quadratic case, the results by Oohama [119] suggest an inner bound which has been proved to be optimal in some cases. A deep analysis along with recent extremal inequalities [97, 136] may yield the expected converse in the general case. However, in the light of known results on Gaussian quadratic multiterminal compression [119, 121, 134, 148, 158], this might be a tricky problem.

Through this chapter, error-free rate-limited links were assumed between the encoders and receivers, while noisy channels could provide additional security, as in the traditional wiretap setting [165]. A result of optimality for the case of degraded channels and side informations has already been derived [106]. The more general setup of *secure transmission of sources over noisy channels with side information at the receivers* is investigated in Chapter 3 hereinafter.

CHAPTER 3

Secure Transmission of Sources over Noisy Channels with Side Information at the Receivers

Abstract. In this chapter, the problem of source-channel coding for secure transmission with arbitrarily correlated side informations at both receivers is investigated. This scenario consists of an encoder (referred to as Alice) that wishes to compress a source and send it through a noisy channel to a legitimate receiver (referred to as Bob). In this context, Alice must simultaneously satisfy the desired requirements on the distortion level at Bob, and the equivocation rate at the eavesdropper (referred to as Eve). This setting can be seen as a generalization of the problems of secure source coding with (uncoded) side information at the decoders (investigated in Section 2.4), and the wiretap channel. A general outer bound on the rate-distortion-equivocation region, as well as an inner bound based on a pure digital scheme, is derived for arbitrary channels and side informations. In some special cases of interest, it is proved that this digital scheme is optimal and that separation holds. However, it is also shown through a simple counterexample with a binary source that a pure analog scheme can outperform the digital one while being optimal. According to these observations and assuming matched-bandwidth, a novel hybrid digital/analog scheme that aims to gather the advantages of both digital and analog ones is then presented. In the quadratic Gaussian setup when side information is only present at the eavesdropper, this strategy is proved to be optimal. Furthermore, it outperforms both digital and analog schemes, and cannot be achieved via time-sharing. By means of an appropriate coding, the presence of any statistical difference among the side informations, the channel noises, and the distortion at Bob can be fully exploited in terms of secrecy.

3.1 Introduction

Consider a system composed of three nodes (or sensors) where each one is measuring an analog source (or random field) as a function of time. One of them (referred to as Alice) wishes to transmit a compressed version of its observation to a second node (referred to as Bob) through a noisy (or wireless) channel. In addition, Bob can use his own observation as side information to decode the received message and refine his estimate of Alice's source. The third node (referred to as Eve) is an eavesdropper i.e., a node that can listen to the messages sent by Alice through another noisy channel. Considering that Eve is not

to be trusted, Alice wishes to leak the smallest amount of information about her source.

Among some major information-theoretic issues, the above scenario involves the notion of secrecy (and its application to source and channel coding), source coding with side information, as well as joint source-channel coding for transmission of sources over noisy channels. The information-theoretic notion of secrecy, introduced by Shannon [140], was first used for secure communication over noisy channels by Wyner [165], who introduced the wiretap channel, further extended by Csiszár and Körner [32]. Extensive research has since been done, yielding several extensions of the original wiretap channel [1, 17, 28, 40, 65, 78, 89, 90, 95, 96, 101, 117]. On the other hand, source coding with side information has been introduced by Slepian and Wolf [143], and Wyner and Ziv [166]. In Chapter 2, we considered such settings with an additional eavesdropper that must be kept as ignorant as possible of the transmitted source (in particular, see Section 2.1 for a review of the literature on this topic).

Most of the existent work separately considers channel or source coding for secure transmission or compression. However, unlike point-to-point communication problems [107, 139], there is no general result of separation for multiterminal settings under security constraints. Recent work [106] considered such a setting of source-channel coding for secure transmission by assuming that Eve has a degraded channel with degraded side information with respect to Bob, and shows that separation holds. This may indicate that *digital* schemes are well-suited for these multiterminal settings with security constraints. On the other hand, it is well-known that *joint* source-channel coding/decoding is a must for broadcast channels without secrecy constraints [47, 155], and hybrid digital/analog schemes have been proved useful for point-to-point problems e.g., to handle SNR mismatch (while they can perform as good as digital or analog ones at the true SNR) [109, 161], as well as for some multiterminal settings [45, 57, 91]. By taking advantage of both analog and digital strategies, they may help to solve the considered problem for secure transmission in the more general case without any degradedness condition.

In this chapter, we consider the setup of joint source-channel coding for secure transmission of a source over a noisy channel with an eavesdropper, and in the presence of side information at the receiving terminals, as depicted in Figure 3.1. This setting can be seen as the unification of the problems of secure source coding with side information at the decoders (investigated in Section 2.4), and the wiretap channel [32, 165]. The main goal is to understand how Alice can take simultaneous advantage of the statistical differences among the side informations and the channel noises to reveal the minimum amount of information to Eve, and satisfy the required distortion level at Bob. It should be emphasized that the central difficulty of this problem lies in the evaluation of the equivocation at Eve. As a matter of fact, the presence of side information at the eavesdropper, that can be used together with its channel output to estimate the source, prevents from directly applying secrecy capacity results [32]. We derive a general outer bound on the achievable region, referred to as the *rate-distortion-equivocation region*, for arbitrary channels and side informations. We then propose a pure digital scheme which combines secure source coding of Chapter 2 with coding for broadcast channels with confidential messages [32], and

derive the corresponding single-letter inner bound. These two bounds do not match in general but we derive two results of optimality when: (*i*) Bob has less noisy side information, and (*ii*) Eve has less noisy channel. In these cases, separation holds and the optimal schemes reduce to a *Wyner-Ziv* source encoder [166] followed by a classical *wiretap* channel encoder [32], and a *secure* source encoder (see Chapter 2) followed by a conventional channel encoder [139], respectively. However, we show through a simple counterexample with a binary source that a pure analog scheme can outperform the digital one while being optimal. Then, restricting our attention to the matched-bandwidth case, we propose a novel hybrid digital/analog scheme that aims to gather the advantages of both digital and analog ones, and derive its single-letter inner bound. In the quadratic Gaussian setup when side information is only present at the eavesdropper, this strategy is proved to be optimal. Furthermore, it outperforms both digital and analog schemes and cannot be achieved via time-sharing. We also consider secure transmission of a binary source with BEC/BSC side informations (as in Section 2.6.2) over a type-II wiretap channel. The proposed hybrid digital/analog scheme turns out to be useful also in this setting.

The rest of this chapter is organized as follows. Section 3.2 states definitions along with the general outer bound on the rate-distortion-equivocation region. Section 3.3 provides a single-letter inner bound based on a digital scheme, as well as special cases where separation holds. The proof of the inner bound is given in Section 3.4. Transmission of a binary source over a type-II wiretap channel is studied in Section 3.5, providing a counterexample for the optimality of the digital scheme. A single-letter inner bound based on a hybrid digital/analog scheme is provided in Section 3.6. The proof is given in Section 3.7. Section 3.8 (resp. Section 3.9) presents an application example to the transmission of a binary source over a type-II wiretap channel (resp. a Gaussian source over a Gaussian wiretap channel with side informations). Section 3.10 concludes the chapter.

Notation

For any sequence $(x_i)_{i\in\mathbb{N}^*}$, notation x_k^n stands for the collection $(x_k, x_{k+1}, \dots, x_n)$. x_1^n is simply denoted by x^n. Entropy is denoted by $H(\cdot)$, and mutual information by $I(\cdot;\cdot)$. We denote typical and conditional typical sets by $T_\delta^n(X)$ and $T_\delta^n(Y|x^n)$, respectively (see Appendix A for details). Let X, Y and Z be three random variables on some alphabets with probability distribution p. If $p(x|yz) = p(x|y)$ for each x, y, z, then they form a Markov chain, which is denoted by $X \multimap Y \multimap Z$. Random variable Y is said to be less noisy than Z w.r.t. X if $I(U;Y) \geq I(U;Z)$ for each random variable U such that $U \multimap X \multimap (Y,Z)$ form a Markov chain. This relation is denoted by $Y \succeq_X Z$. The set of nonnegative real numbers is denoted by $\mathbb{R}_+$. For each $x \in \mathbb{R}$, notation $[x]_+$ stands for $\max\{0\,;x\}$. Logarithms are taken in base 2 and denoted by $\log(\cdot)$. The binary entropy function is defined on $[0,1]$ as $h_2(x) = -x\log(x) - (1-x)\log(1-x)$. Its inverse h_2^{-1} is defined on $[0,1]$ and takes values in $[0,\frac{1}{2}]$. For each $a, b \in [0,1]$, $a \star b = a(1-b) + (1-a)b$. The Bernoulli distribution of parameter u is denoted by $\mathcal{B}(u)$.

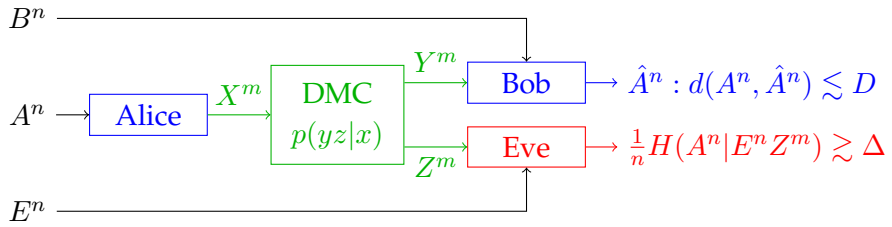


Figure 3.1: Secure transmission with side information at the receivers.

3.2 Problem definition and general outer bound

3.2.1 Problem definition

In this section, we give a more rigorous formulation of the context depicted in Figure 3.1. Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{E}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be six finite sets. Alice, Bob, and Eve observe the sequences of random variables $(A_i)_{i\in\mathbb{N}^*}$, $(B_i)_{i\in\mathbb{N}^*}$, and $(E_i)_{i\in\mathbb{N}^*}$, respectively, which take values on $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{E}$, resp. For each $i \in \mathbb{N}^*$, the random variables A_i, B_i, and E_i are distributed according to the joint distribution $p(abe)$ on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$. Moreover, they are independent across time i. Alice can also communicate with Bob and Eve through a discrete memoryless channel with input X on $\mathcal{X}$, and outputs Y, Z on $\mathcal{Y}$, $\mathcal{Z}$, respectively. This channel is defined by its transition probability $p(yz|x)$.

Let $d\colon \mathcal{A}\times\mathcal{A} \to [0, d_{\max}]$ be a finite distortion measure i.e., such that $0 \leq d_{\max} < \infty$. We also denote by d the component-wise mean distortion on $\mathcal{A}^n \times \mathcal{A}^n$ i.e., for each $a^n, b^n \in \mathcal{A}^n$, $d(a^n, b^n) = \frac{1}{n}\sum_{i=1}^n d(a_i, b_i)$.

Definition 3.1 (Code)**.** An (n, m)-code for source-channel coding is defined by

- a (stochastic) encoding function at Alice $F\colon \mathcal{A}^n \to \mathcal{X}^m$, defined by some transition probability $P_F(x^m|a^n)$,
- a decoding function at Bob $g\colon \mathcal{B}^n \times \mathcal{Y}^m \to \mathcal{A}^n$.

The rate of such a code is defined as the number of channel uses per source symbol $\frac{m}{n}$.

Definition 3.2 (Achievability)**.** A tuple $(k, D, \Delta) \in \mathbb{R}_+^3$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an (n, m)-code (F, g) such that:

$$\begin{aligned} \frac{m}{n} &\leq k + \varepsilon \,, \\ \mathbb{E}\big[d(A^n, g(B^n, Y^m))\big] &\leq D + \varepsilon \,, \\ \frac{1}{n} H(A^n|E^n Z^m) &\geq \Delta - \varepsilon \,, \end{aligned}$$

with channel input X^m as the output of the encoder $F(A^n)$.
The set of all achievable tuples is denoted by $\mathcal{R}^*$ and is referred to as the *rate-distortion-equivocation region*.

Remark 3.1. Region $\mathcal{R}^*$ is closed and convex.

Remark 3.2. Quantities involved in Definition 3.2 only depend on the marginal distributions $p(ae)$, $p(ab)$, $p(y|x)$ and $p(z|x)$. The same applies for subsequent results that provide inner and outer bounds on $\mathcal{R}^*$.

3.2.2 General outer bound

The following theorem gives an outer bound on $\mathcal{R}^*$ i.e., it defines region $\mathcal{R}_{\text{out}} \supseteq \mathcal{R}^*$.

Theorem 3.1 (Outer bound). *If (k, D, Δ) is achievable, then there exist random variables U, V, Q, T, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$, respectively, with joint distribution $p(uvqtabexyz) = p(uv|a)p(abe)\, p(q|t)p(t)p(x|t)p(yz|x)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, verifying the following inequalities:*

$$I(V; A|B) \leq kI(T; Y)\,, \tag{3.1}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big]\,, \tag{3.2}$$

$$\Delta \leq H(A|UE) - \Big[I(V; A|B) - I(U; A|B) - k\Big(I(T; Y|Q) - I(T; Z|Q)\Big)\Big]_+\,. \tag{3.3}$$

Proof. See Appendix E.1. □

3.3 Digital scheme

In this section, we propose a digital coding scheme for secure transmission with side information and derive the corresponding single-letter inner bound $\mathcal{R}_{\text{digital}}$ (Theorem 3.2). This scheme turns out to be optimal under some less-noisy conditions (Propositions 3.3 and 3.4).

3.3.1 General statement

The following theorem gives an inner bound on $\mathcal{R}^*$ i.e., it defines region $\mathcal{R}_{\text{digital}} \subseteq \mathcal{R}^*$. The achievability follows by combining secure source coding of Chapter 2 with coding for broadcast channels with confidential messages [32]. This scheme will be referred to as the *digital scheme*.

Theorem 3.2 (Digital scheme). *A tuple $(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist random variables U, V, Q, T, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$, respectively, with joint distribution $p(uvqtabexyz) = p(u|v)p(v|a)p(abe)\, p(q|t)p(t)p(x|t)p(yz|x)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, verifying the following inequalities:*

$$I(U; A|B) \leq kI(Q; Y)\,, \tag{3.4}$$

$$I(V; A|B) \leq kI(T; Y)\,, \tag{3.5}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big]\,, \tag{3.6}$$

$$\Delta \leq H(A|UE) - \Big[I(V; A|UB) - k\Big(I(T; Y|Q) - I(T; Z|Q)\Big)\Big]_+\,. \tag{3.7}$$

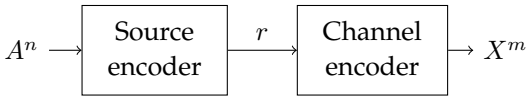


Figure 3.2: Traditional separation.

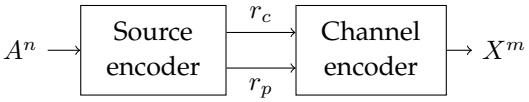


Figure 3.3: Proposed system ("operational" separation).

Proof. See Section 3.4. □

Inequalities (3.4), (3.5) correspond to sufficient conditions for the transmission of two source layers U, V in channel variables Q, T, respectively. The first layer (U, Q) can be seen as a *common* message which is considered to be known at Eve, as shown by the term $H(A|UE)$ in (3.7). The second layer (V, T) forms a *private* message which is (partially) protected by adding an independent random noise [32, 90]. The term in square brackets in (3.7) corresponds to the information that Eve can still obtain on this protected layer.

Notice that the inner and outer bounds $\mathcal{R}_{\text{digital}}$ and $\mathcal{R}_{\text{out}}$ do not meet in general:

- Condition (3.4) in Theorem 3.2, which is needed in our scheme to characterize the equivocation at Eve, may not be optimal in the general case (see Theorem 3.1).
- The Markov chain $U \multimap V \multimap A \multimap (B, E)$ is assumed in Theorem 3.2 while only $(U, V) \multimap A \multimap (B, E)$ is proved for arbitrary codes in Theorem 3.1.

We provide in Section 3.3.3 several cases where $\mathcal{R}_{\text{digital}}$ is optimal.

3.3.2 Coding scheme based on "operational" separation

In traditional *separated* schemes, two *stand-alone* components successively perform source and channel coding, as depicted in Figure 3.2. However the scheme that achieves region $\mathcal{R}_{\text{digital}}$ does not satisfy this separation principle: The source encoder outputs two layers which are further encoded by using the channel code for a broadcast channel with confidential messages [32] (see Section 3.4). This results in two independent (but not stand-alone) source and channel components yielding statistically independent source and channel variables (as in [155] for Slepian-Wolf coding over broadcast channels) i.e., "operational" separation holds (see Figure 3.3). As a matter of fact, inequality (3.4) in Theorem 3.2 prevents from separately choosing variables U and Q which would maximize the equivocation rate at Eve (3.7).

3.3.3 Special cases

In this section, we characterize the optimality of the inner bound $\mathcal{R}_{\text{digital}}$ for some special cases.

3.3.3.1 Bob has less noisy side information

If Bob has less noisy side information than Eve i.e., $B \succeq_A E$, the optimal coding scheme reduces to a *Wyner-Ziv* source encoder [166] followed by a classical *wiretap* channel encoder [32], and hence separation holds (Figure 3.2):

Proposition 3.3. *If $B \succeq_A E$, $(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if and only if there exist random variables V, Q, T, X on finite sets $\mathcal{V}$, $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{X}$, respectively, with joint distribution $p(vqtabexyz) = p(v|a)p(abe)\,p(q|t)p(t)p(x|t)p(yz|x)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, verifying*

$$\begin{aligned} &I(V;A|B) \leq kI(T;Y)\,, \\ &D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\,, \\ &\Delta \leq H(A|E) - \Big[I(V;A|B) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+ . \end{aligned}$$

Proof. The above region is achievable by setting variable U to a constant value in Theorem 3.2. On the other hand, the third inequality of Theorem 3.1 writes:

$$\begin{aligned} &\Delta \leq H(A|UE) \\ &\Delta \leq H(A|VB) + I(A;B|U) - I(A;E|U) + k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\,. \end{aligned}$$

Since $B \succeq_A E$, and $U \multimap A \multimap (B,E)$ form a Markov chain, $I(A;B|U) - I(A;E|U) \leq I(A;B) - I(A;E)$. Moreover $H(A|UE) \leq H(A|E)$. In this case, the outer bound $\mathcal{R}_{\text{out}}$ is thus included in (and consequently equal to) $\mathcal{R}_{\text{digital}}$. □

If the informations at Eve (both side information, and channel output) are degraded versions of Bob's ones i.e., if both Markov chains $A \multimap B \multimap E$, and $X \multimap Y \multimap Z$ hold, then Proposition 3.3 reduces to the results in [106]. In this case, variable Q is set to a constant value, and $T = X$.

3.3.3.2 Eve has less noisy channel

If Eve has less noisy channel than Bob i.e., $Z \succeq_X Y$, the optimal scheme reduces to a *secure* source encoder (see Chapter 2) followed by a conventional channel encoder [139], and hence separation holds (Figure 3.2):

Proposition 3.4. *If $Z \succeq_X Y$, $(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if and only if there exist random variables U, V, X on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, respectively, with joint distribution $p(uvabexyz) = p(u|v)p(v|a)p(abe)\,p(x)p(yz|x)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, verifying*

$$\begin{aligned} &I(V;A|B) \leq kI(X;Y)\,, \\ &D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]\,, \\ &\Delta \leq H(A|VB) + I(A;B|U) - I(A;E|U)\,. \end{aligned}$$

Proof. The above region is achievable by setting $Q = T = X$ in Theorem 3.2. A new proof is needed to obtain the converse part. Here, auxiliary variables are defined as follows, for each $i \in \{1, \dots, n\}$, and each $j \in \{1, \dots, m\}$:

$$\begin{aligned} U_i &= (\qquad\qquad B_{i+1}^n, E^{i-1}, Y^m) \,, \\ V_i &= (A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1}, Y^m) \,, \\ Q_j &= (\quad E^n, Y^{j-1}, Z_{j+1}^m) \,, \\ T_j &= (A^n, E^n, Y^{j-1}, Z_{j+1}^m) \,. \end{aligned}$$

Now, both $U_i \multimap V_i \multimap A_i \multimap (B_i, E_i)$, and $Q_j \multimap T_j \multimap X_j \multimap (Y_j, Z_j)$ form Markov chains (see Figure E.1). Following the arguments given in Appendix E.1, we can define new variables U, V, Q, T verifying the above Markov chains and the following inequalities:

$$\begin{aligned} & I(V; A|B) \leq kI(T; Y) \,, \\ & D \geq \mathbb{E}\big[d(A, \hat{A}(V, B))\big] \,, \\ & \Delta \leq H(A|UE) - I(V; A|UB) + k\Big(I(T; Y|Q) - I(T; Z|Q)\Big). \end{aligned}$$

Since $Z \succeq_X Y$, and $Q \multimap T \multimap X \multimap (Y, Z)$ form a Markov chain, $I(T; Y|Q) - I(T; Z|Q) \leq 0$ and $I(T; Y) \leq I(X; Y)$. This concludes the proof. □

3.3.3.3 Secure source coding

Defining the transmitted rate as $R = kI(X; Y)$, Proposition 3.4 provides the single-letter characterization of the *rate-distortion-equivocation* region in the setup of secure source coding with uncoded side information given in Theorem 2.6.

3.3.3.4 Wiretap channel

Choosing appropriate side informations and auxiliary variables, region $\mathcal{R}_{\text{digital}}$ reduces to the achievable region for the wiretap channel [90, Eq. (2.6)].

3.4 Proof of Theorem 3.2 (Digital scheme)

Let U, V, Q, X be four random variables on finite sets $\mathcal{U}, \mathcal{V}, \mathcal{Q}, \mathcal{X}$, respectively, such that $p(uvqabexyz) = p(u|v)p(v|a)p(abe)\, p(q|x)p(x)p(yz|x)$, a function $\hat{A} \colon \mathcal{V} \times \mathcal{B} \to \mathcal{A}$, and a tuple $(k, D, \Delta) \in \mathbb{R}_+^3$. In this section, we describe a scheme that achieves (under some sufficient conditions) tuple (k, D, Δ) i.e., for any $\varepsilon > 0$, we construct an (n, m)-code (F, g) such that:

$$\begin{aligned} \frac{m}{n} &\leq k + \varepsilon \,, \\ \mathbb{E}\big[d\big(A^n, g(B^n, Y^m)\big)\big] &\leq D + \varepsilon \,, \\ \frac{1}{n} H(A^n|E^n Z^m) &\geq \Delta - \varepsilon \,. \end{aligned}$$

In this scheme, Alice compresses the source A in descriptions (U, V), with V on the top of U. In view of the side information at Bob B, random binning a la Wyner-Ziv [166] is performed. The corresponding bin indices (r_1, r_2) are then mapped to indices (r_c, r_p), which are further transmitted to Bob through variables (Q, X) using a code for broadcast channel with confidential messages [32], where index r_p is protected by an independent random noise r_f. As in the classical wiretap channel [32, 90], its rate R_f satisfies some constraint that allows to characterize the equivocation rate at Eve.

Let $\varepsilon > 0$, $R_1, R_2, R_c, R_p, R_f \in \mathbb{R}_+^*$, $S_1 \geq R_1$, $S_2 \geq R_2$ such that

$$R_f < (k + \varepsilon)\, I(X; Z|Q)\ , \tag{3.8}$$

and assume that a local (independent and uniformly distributed) random source with rate R_f is available at Alice. Define $\gamma = \frac{\varepsilon}{9\, d_{\max}}$.

3.4.1 Codebook generation

3.4.1.1 Source codewords

Randomly pick 2^{nS_1} sequences $u^n(s_1)$ from $T_\delta^n(U)$ and divide them into 2^{nR_1} equal size bins $B_1(r_1)$, $r_1 \in \{1, \ldots, 2^{nR_1}\}$. Then, for each codeword $u^n(s_1)$, randomly pick 2^{nS_2} sequences $v^n(s_1, s_2)$ from $T_\delta^n(V|u^n(s_1))$ and divide them into 2^{nR_2} equal size bins $B_2(s_1, r_2)$, $r_2 \in \{1, \ldots, 2^{nR_2}\}$. See Figure 3.4.

3.4.1.2 Channel codewords

Randomly pick 2^{nR_c} sequences $q^m(r_c)$ from $T_\delta^m(Q)$. Then, for each codeword $q^m(r_c)$, randomly pick $2^{n(R_p+R_f)}$ sequences $x^m(r_c, r_p, r_f)$ from $T_\delta^m(X|q^m(r_c))$. See Figure 3.5.

3.4.2 Encoding procedure

Assume that source sequence A^n and random noise r_f are produced at Alice.

Look for the first codeword $u^n(s_1)$ such that $(u^n(s_1), A^n) \in T_\delta^n(U, A)$. Then look for a codeword $v^n(s_1, s_2)$ such that $(v^n(s_1, s_2), A^n) \in T_\delta^n(V, A|u^n(s_1))$. Let $B_1(r_1)$ and $B_2(s_1, r_2)$ be the bins of $u^n(s_1)$ and $v^n(s_1, s_2)$, respectively.

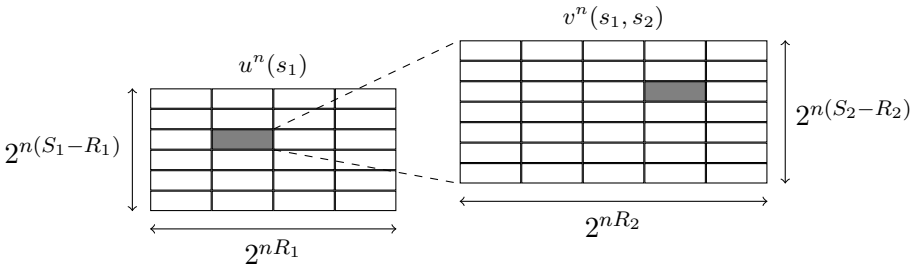


Figure 3.4: Digital scheme–Source codebook.

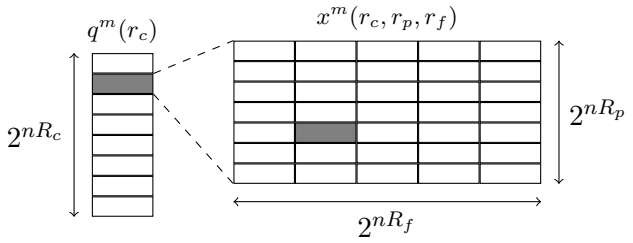


Figure 3.5: Digital scheme–Channel codebook.

Define $(r_c, r_p) = M(r_1, r_2) \in \{1, \ldots, 2^{nR_c}\} \times \{1, \ldots, 2^{nR_p}\}$ where M is an arbitrary fixed one-to-one mapping such that $r_1 = M'(r_c)$ for some mapping M'. These two functions can be defined if:

$$R_1 + R_2 = R_c + R_p \,, \tag{3.9}$$

$$R_1 \leq R_c \,. \tag{3.10}$$

Alice then sends $X^m = F(A^n) \triangleq x^m(r_c, r_p, r_f)$.

3.4.3 Decoding procedure

Assume that Bob observes B^n and receives Y^m from Alice.

Look for the unique codeword $q^m(r_c)$ such that $(q^m(r_c), Y^m) \in T_\delta^m(Q, Y)$. Then look for the unique codeword $x^m(r_c, r_p, r_f)$ such that $(x^m(r_c, r_p, r_f), Y^m) \in T_\delta^m(X, Y|q^m(r_c))$.

Compute $(r_1, r_2) = M^{-1}(r_c, r_p)$.

Look for the unique codeword $u^n(s_1) \in B_1(r_1)$ such that $(u^n(s_1), B^n) \in T_\delta^n(U, B)$. Then look for the unique codeword $v^n(s_1, s_2) \in B_2(s_1, r_2)$ such that $(v^n(s_1, s_2), B^n) \in T_\delta^n(V, B|u^n(s_1))$.

Compute the estimate $g(B^n, Y^m) \in \mathcal{A}^n$ using the following component-wise relation, for each $i = \{1, \ldots, n\}$:

$$g_i(B^n, Y^m) \triangleq \hat{A}(v_i(s_1, s_2), B_i) \,.$$

3.4.4 Errors and constraints

Denoting by E the event "An error occurred during the encoding or decoding steps," we expand its probability (averaged over the set of all possible codebooks) as follows: $\Pr\{\mathsf{E}\} \leq P_{t,1} + P_{t,2} + P_{e,1} + P_{e,2} + P_{d,1} + P_{d,2} + P_{d,3} + P_{d,4}$, where each term corresponds to a particular error event, as detailed below. We derive sufficient conditions on the parameters that make each of these probabilities small for some sufficiently large n. From now on, let $m = \lfloor n(k + \varepsilon) \rfloor$.[1]

[1]Note that $m \to \infty$ as $n \to \infty$.

3.4.4.1 Typicality

From standard properties of typical sequences (see Appendix A), there exists a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that $P_{t,1} \triangleq \Pr\{(A^n, B^n, E^n) \notin T_\delta^n(A, B, E)\} \leq \eta_n$. Consequently, $P_{t,1} \leq \gamma$ for some sufficiently large n.

Similarly, since the input of the channel X^m is set to some codeword $x^m(r_c, r_p, r_f) \in T_\delta^m(X)$, $P_{t,2} \triangleq \Pr\{(X^m, Y^m, Z^m) \notin T_\delta^m(X, Y, Z)\} \leq \gamma$ for some sufficiently large n.

3.4.4.2 Encoding

In the first encoding step, Alice needs to find (at least) one codeword $u^n(s_1)$ such that $(u^n(s_1), A^n) \in T_\delta^n(U, A)$. Following the argument of Section 2.3.4.2, we can prove that if $S_1 > I(U; A)$, then the probability that this step fails $P_{e,1}$ can be upper bounded by γ for some sufficiently large n.

Similarly, the second encoding step succeeds with probability $1 - P_{e,2} \geq 1 - \gamma$ under condition $S_2 > I(V; A|U)$.

3.4.4.3 Decoding indices

In the first decoding step, Bob looks for the *unique* codeword $q^m(r_c)$ such that $(q^m(r_c), Y^m) \in T_\delta^m(Q, Y)$. Following standard argument for channel coding, we can prove that if $R_c < (k + \varepsilon)I(Q; Y)$, then the probability that there exists another admissible codeword $P_{d,1}$ can be lowered below γ for some sufficiently large n.

Similarly, the second encoding step succeeds with probability $1 - P_{d,2} \geq 1 - \gamma$ under condition $R_p + R_f < (k + \varepsilon)I(X; Y|Q)$.

3.4.4.4 Decoding source variables

In the third decoding step, Bob looks for the *unique* codeword $u^n(s_1) \in B_1(r_1)$ such that $(u^n(s_1), B^n) \in T_\delta^n(U, B)$. Following standard argument for source coding (see e.g. Section 2.3.4.4 and Appendix D.1), we can prove that if $S_1 - R_1 < I(U; B)$, then the probability that there exists another admissible codeword $P_{d,3}$ can be lowered below γ for some sufficiently large n.

Similarly, the fourth decoding step succeeds with probability $1 - P_{d,4} \geq 1 - \gamma$ under condition $S_2 - R_2 < I(V; B|U)$.

3.4.4.5 Summary

In this paragraph, we proved that under some sufficient conditions, $\Pr\{\mathsf{E}\} \leq 8\gamma$.

3.4.5 Distortion at Bob

We now check that our code achieves the required distortion level at Bob (averaged over the set of all possible codebooks):

$$\begin{aligned}\mathbb{E}\Big[d\big(A^n, g(B^n, Y^m)\big)\Big] &\leq (1-\Pr\{\mathsf{E}\})\mathbb{E}\left[d\big(A^n, \hat{A}\big(v^n(s_1,s_2), B^n\big)\big)\middle|\cancel{\mathsf{E}}\right] + \Pr\{\mathsf{E}\}\, d_{\max} \\ &\leq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] + \frac{\varepsilon}{9} + \frac{8\varepsilon}{9}\,,\end{aligned}$$

where the last inequality holds for some sufficiently large n, and follows from $\Pr\{\mathsf{E}\} \leq 8\gamma$, the definition of γ, and the argument given in Section 2.3.5.

Condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big]$ is thus sufficient to achieve distortion $D+\varepsilon$ at Bob.

3.4.6 Equivocation rate at Eve

In the following paragraphs, we prove a lower bound on the equivocation rate at Eve. We first split up the equivocation into two terms which will be studied separately:

$$H(A^n|E^nZ^m) = \underbrace{H(A^n|r_c r_p E^n Z^m)}_{E_s} + \underbrace{I(A^n; r_c r_p|E^n Z^m)}_{E_c}\,. \tag{3.11}$$

3.4.6.1 Study of E_s

The "source" term E_s writes:

$$\begin{aligned}E_s &\overset{(a)}{=} H(A^n|r_1 r_2 E^n) \\ &\overset{(b)}{=} H(A^n|r_1 E^n) - H(r_2|r_1 E^n) \\ &= H(A^n|r_1 E^n) - H(r_2) + I(r_2; r_1 E^n) \\ &\overset{(c)}{\geq} nH(A|UE) - n\,\tfrac{\varepsilon}{4} - nR_2 + I(r_2; E^n|r_1)\,,\end{aligned} \tag{3.12}$$

where

- step (a) follows from the Markov chain $A^n \multimap (r_c, r_p, E^n) \multimap Z^m$ and the identity $(r_c, r_p) = M(r_1, r_2)$ where M is a one-to-one mapping,
- step (b) from the fact that the bin index r_2 is a deterministic function of A^n,
- step (c) from Lemma 2.5 (for some sufficiently large n), the fact that $r_2 \in \{1, \ldots, 2^{nR_2}\}$, and the non-negativity of mutual information.

Note that this term corresponds to the one previously studied in Section 2.3.6. The above lower bound should however be tighter than (2.12) since we do not neglect the remainder term $I(r_2; E^n|r_1)$.

3.4.6.2 Study of E_c

The "channel" term E_c writes:

$$\begin{aligned} E_c &= H(r_c r_p | E^n Z^m) \\ &= H(r_p | r_c Z^m) + H(r_c | Z^m) - I(r_c r_p; E^n | Z^m) \,, \end{aligned} \tag{3.13}$$

where the first step follows from the fact that (r_c, r_p) is a deterministic function of A^n.

The first term of the r.h.s. of (3.13) corresponds to the equivocation (of the *private* message, given the *common* message and the output of the channel) in the wiretap channel setting. Following the arguments of [32, Section IV], [90, Section 2.3],[2] we can easily prove the following lower bound:

$$H(r_p | r_c Z^m) \geq n(R_p + R_f) - mI(X; Z|Q) - 1 - n\,\tfrac{\varepsilon}{2} \,, \tag{3.14}$$

for some sufficiently large m.

3.4.6.3 End of proof

Gathering (3.11)–(3.14), we proved that:

$$\begin{aligned} H(A^n | E^n Z^m) \geq\; & nH(A|UE) - nR_2 + n(R_p + R_f) - mI(X; Z|Q) \\ & + I(r_2; E^n | r_1) + H(r_c | Z^m) - I(r_c r_p; E^n | Z^m) - n\,\tfrac{3\varepsilon}{4} - 1 \,. \end{aligned} \tag{3.15}$$

We now study the remainder of the r.h.s. of the above inequality:

$$\begin{aligned} & I(r_2; E^n | r_1) + H(r_c | Z^m) - I(r_c r_p; E^n | Z^m) \\ & \quad = I(r_1 r_2; E^n) - I(r_1; E^n) + H(r_c | Z^m) - I(Z^m r_c r_p; E^n) + I(Z^m; E^n) \\ & \quad \overset{(a)}{=} - I(r_1; E^n) + H(r_c | Z^m) + I(Z^m; E^n | r_c r_p) + I(Z^m; E^n) \\ & \quad \overset{(b)}{\geq} - I(r_1; E^n) + I(r_c Z^m; E^n) + H(r_c | E^n Z^m) \\ & \quad \overset{(c)}{\geq} 0 \,, \end{aligned}$$

where

- step (a) follows from the identity $(r_c, r_p) = M(r_1, r_2)$ where M is a one-to-one mapping,
- step (b) from the non-negativity of conditional mutual information,

[2] The proof relies on (*i*) definition $X^m = x^m(r_c, r_p, r_f)$, (*ii*) the fact that codewords $x^m(r_c, r_p, r_f)$ are *nearly uniformly* distributed (given r_c) over a set of cardinality $2^{n(R_p+R_f)}$, (*iii*) the fact that the channel $X \mapsto Z$ is memoryless, (*iv*) Fano's inequality together with constraint (3.8), which ensures that Eve can decode $x^m(r_c, r_p, r_f)$ from (r_p, r_f) with an arbitrarily small probability of error, (*v*) standard properties of typical sequences, and (*vi*) the Markov chain $Q \multimap X \multimap Z$.

- step (c) from the fact that $r_1 = M'(r_c)$ for some mapping M', and the non-negativity of conditional entropy and mutual information.

Inequality (3.15) then yields

$$\frac{1}{n}H(A^n|E^nZ^m) \geq H(A|UE) - R_2 + R_p + R_f - \frac{m}{n}\,I(X;Z|Q) - \varepsilon\,,$$

for some sufficiently large n.

Condition $\Delta \leq H(A|UE) - R_2 + R_p + R_f - (k+\varepsilon)I(X;Z|Q)$ is thus sufficient to achieve equivocation rate $\Delta - \varepsilon$.

3.4.7 Summary of sufficient conditions

Putting all pieces together, we proved that the following inequalities are sufficient conditions for a tuple $(k, D, \Delta) \in \mathbb{R}_+^3$ to be achievable: For each $\varepsilon > 0$,

$$\begin{cases} R_1, R_2, R_c, R_p, R_f > 0 \\ R_1 + R_2 = R_c + R_p \\ \quad R_1 \leq R_c \\ \quad S_1 \geq R_1 \\ \quad S_2 \geq R_2 \\ \quad S_1 > I(U;A) \\ \quad S_2 > I(V;A|U) \\ \quad R_c < (k+\varepsilon)I(Q;Y) \\ R_p + R_f < (k+\varepsilon)I(X;Y|Q) \\ S_1 - R_1 < I(U;B) \\ S_2 - R_2 < I(V;B|U) \\ \quad R_f < (k+\varepsilon)I(X;Z|Q) \\ \quad D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] \\ \quad \Delta \leq H(A|UE) - R_2 + R_p + R_f - (k+\varepsilon)I(X;Z|Q) \end{cases}$$

Using Fourier-Motzkin elimination [156], it is straightforward to prove that this system of inequalities is equivalent to:

$$\begin{cases} I(U;A|B) < (k+\varepsilon)I(Q;Y) \\ I(V;A|B) < (k+\varepsilon)I(X;Y) \\ \quad D \geq \mathbb{E}\big[d(A, \hat{A}(V,B))\big] \\ \quad \Delta < H(A|UE) \\ \quad \Delta < H(A|UE) - I(V;A|UB) + (k+\varepsilon)\Big(I(X;Y|Q) - I(X;Z|Q)\Big) \end{cases}$$

3.4.8 Channel prefixing

For each random variable T on some finite set $\mathcal{T}$ such that $T \multimap X \multimap (Y,Z)$ form a Markov chain, we can use the above scheme considering the DMC $T \mapsto (Y,Z)$ instead of $X \mapsto (Y,Z)$. In this case, the above sufficient conditions write

$$\begin{cases} I(U;A|B) < (k+\varepsilon) I(Q;Y) \\ I(V;A|B) < (k+\varepsilon) I(T;Y) \\ \qquad D \geq \mathbb{E}\big[d(A,\hat{A}(V,B))\big] \\ \qquad \Delta < H(A|UE) \\ \qquad \Delta < H(A|UE) - I(V;A|UB) + (k+\varepsilon)\Big(I(T;Y|Q) - I(T;Z|Q)\Big) \end{cases}$$

Since region $\mathcal{R}^*$ is closed, this proves Theorem 3.2. □

3.5 Secure transmission of a binary source with BEC/BSC side informations over a type-II wiretap channel

3.5.1 System model

Consider the source model introduced in Section 2.6.2 and depicted in Figure 3.6, where the source is binary uniformly distributed ($A \sim \mathcal{B}\left(\frac{1}{2}\right)$) and the side information at Bob, resp. Eve, is the output of a binary erasure channel (BEC) with erasure probability $\beta \in (0,1]$, resp. a binary symmetric channel (BSC) with crossover probability $\epsilon \in [0, \frac{1}{2}]$, with input A.

Recall that according to the values of the parameters (β, ϵ), the side informations satisfy the properties summarized in Figure 3.8 [112].

The communication channel is similar to the type-II wiretap channel of [165]: It consists of a noiseless channel from Alice to Bob, and a BSC with crossover probability $\zeta \in [0, \frac{1}{2}]$, from Alice to Eve (see Figure 3.7).

In this section, we focus on *lossless* reconstruction at Bob (d is the Hamming distance and $D = 0$) and *matched bandwidth* ($k = 1$).

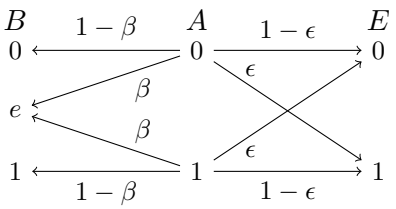


Figure 3.6: Binary source with BEC/BSC side informations.

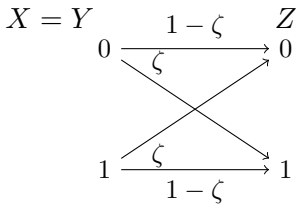


Figure 3.7: Type-II wiretap channel.

3.5.2 Performance of coding schemes

From the general outer bound of Theorem 3.1, we can easily derive the following result.

Proposition 3.5 (Outer bound). *If $(k = 1, D = 0, \Delta)$ is achievable, then there exist $u, q \in [0, \frac{1}{2}]$ such that*

$$\Delta \leq h_2(\epsilon) + h_2(u) - h_2(\epsilon \star u) - \Big[\beta h_2(u) - \Big(h_2(\zeta) + h_2(q) - h_2(\zeta \star q)\Big)\Big]_+ .$$

Proof. The proof is similar to the one of the converse part of Proposition 3.6 below, given in Appendix E.2. Details are omitted. □

The following proposition provides a simple expression of region $\mathcal{R}_{\text{digital}}$.

Proposition 3.6 (Digital scheme). $(k = 1, D = 0, \Delta) \in \mathcal{R}_{digital}$ *if and only if there exist $u, q \in [0, \frac{1}{2}]$ such that*

$$\beta(1 - h_2(u)) \leq 1 - h_2(q) ,$$
$$\Delta \leq h_2(\epsilon) + h_2(u) - h_2(\epsilon \star u) - \Big[\beta h_2(u) - \Big(h_2(\zeta) + h_2(q) - h_2(\zeta \star q)\Big)\Big]_+ .$$

Proof. The proof of the converse part is given in Appendix E.2.

The direct part follows from Theorem 3.2 after some straightforward manipulations choosing auxiliary variables as follows (details are omitted): $V = A$; $X \sim \mathcal{B}\left(\frac{1}{2}\right)$; U (resp. Q) is the output of a BSC with crossover probability $u \in [0, \frac{1}{2}]$ (resp. $q \in [0, \frac{1}{2}]$) and input A (resp. X). □

Notice that if $\beta \leq 4\epsilon(1 - \epsilon)$, then $B \succeq_A E$, and hence Proposition 3.3 holds i.e., the above inner bound is optimal and separation holds.

In the following, we will compare the above digital scheme with a pure analog one, consisting in directly sending the source over the channel. Its performance is given by the following proposition.

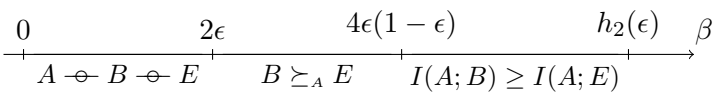


Figure 3.8: Relative properties of the side informations as a function of (β, ϵ).

Proposition 3.7 (Analog scheme). *A tuple* $(k = 1, D = 0, \Delta) \in \mathbb{R}_+^3$ *is achievable through an analog scheme if*

$$\Delta \leq h_2(\epsilon) + h_2(\zeta) - h_2(\zeta \star \epsilon) \, .$$

Proof. Letting $X = A$ yields zero distortion at Bob (since $Y = X$) and equivocation rate $H(A|EZ)$ at Eve. The above expression follows after some straightforward manipulations. Details are omitted. □

3.5.3 Counterexample for the optimality of Theorem 3.2

Let now assume that Bob does not have any side information i.e., $B = \emptyset$ or equivalently $\beta = 1$, and let $\epsilon = \zeta = 0.1$, so that $A \multimap E \multimap B$ and $X \multimap Y \multimap Z$ form Markov chains, and neither Proposition 3.3, nor Proposition 3.4 applies.

This setting provides a counterexample for the general optimality of the inner bound in Theorem 3.2: Numerical optimization over u and q in Proposition 3.6 indicates that the proposed digital scheme achieves an equivocation rate $\Delta = 0.056$, while the naive analog scheme of Proposition 3.7 achieves $\Delta = 0.258$. Furthermore, the latter coincides with the outer bound of Proposition 3.5. This shows that a *joint* source-channel scheme may achieve better performance in some cases.

3.6 Hybrid coding

Based on the observations of the previous section about the usefulness of *analog schemes*, we propose in this section a *hybrid digital/analog scheme* that yields a new single-letter inner bound $\mathcal{R}_{\text{hybrid}}$ in the matched-bandwidth case (Theorem 3.8).

3.6.1 General statement

Channels $A \mapsto B$ and $X \mapsto Y$ can be viewed together as a state-dependent channel with input X, state A and output (B, Y). In this perspective, Alice and Bob form a communication system with channel state information non-causally known at the transmitter (CSIT), as depicted in Figure 3.9. Roughly speaking, the proposed scheme consists in sending independent digital random noise r_f using a Gelfand-Pinsker code [48] for this equivalent state-dependent channel.

Theorem 3.8 (Hybrid scheme). *A tuple* $(k = 1, D, \Delta) \in \mathbb{R}_+^3$ *is achievable if there exist random variables* U, V, X *on finite sets* $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, *with joint distribution* $p(uvabexyz) = p(u|v)\, p(vx|a)\, p(abe)p(yz|x)$, $x = x(v, a)$, *and a function* $\hat{A} \colon \mathcal{V} \times \mathcal{B} \times \mathcal{Y} \to \mathcal{A}$, *verifying*

$$I(U; A) \leq I(U; BY) \, , \tag{3.16}$$

$$I(V; A|U) \leq I(V; BY|U) \, , \tag{3.17}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] \, , \tag{3.18}$$

$$\Delta \leq H(A|UE) - I(V; A|U) - I(X; Z|UE) + \min\Big\{I(V; BY|U)\,; I(V; AZ|U)\Big\} \, . \tag{3.19}$$

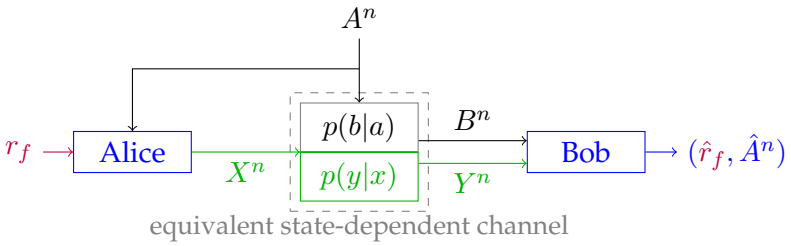


Figure 3.9: Alice and Bob as a system with state-dependent channel and CSIT.

Proof. See Section 3.7. □

Inequalities (3.16), (3.17) correspond to sufficient conditions for the transmission of descriptions U, V of A. The first layer U can be seen as a *common* message which is considered to be known at Eve, as shown by the term $H(A|UE)$ in (3.19). Digital random noise r_f helps to secure the second layer V against Eve.

3.6.2 Special cases

3.6.2.1 Analog schemes

The proposed scheme can reduce to a pure analog one (as the simple one of Proposition 3.7). Hence, $\mathcal{R}_{\text{hybrid}}$ contains tuples that may not be in $\mathcal{R}_{\text{digital}}$: $\mathcal{R}_{\text{hybrid}} \not\subset \mathcal{R}_{\text{digital}}$.

3.6.2.2 Digital schemes

By defining the variables in Theorem 3.8 as pairs of independent source and channel components, we can obtain the structure of those in Theorem 3.2, but such variables do not verify all inequalities and thus $\mathcal{R}_{\text{digital}} \not\subset \mathcal{R}_{\text{hybrid}}$.

3.6.2.3 Wiretap channel

Choosing independent source and channel variables with appropriate rates, region $\mathcal{R}_{\text{hybrid}}$ reduces to the achievable region for the wiretap channel [90, Eq. (2.6)].

3.7 Proof of Theorem 3.8 (Hybrid scheme)

Let U, V, X be three random variables on finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{X}$, respectively, such that $p(uvabexyz) = p(u|v)p(vx|a)p(abe)p(yz|x)$, $x = x(v,a)$, a function $\hat{A}\colon \mathcal{V} \times \mathcal{B} \times \mathcal{Y} \to \mathcal{A}$, and a tuple $(D, \Delta) \in \mathbb{R}_+^2$. In this section, we describe a scheme that achieves (under some sufficient conditions) tuple $(k = 1, D, \Delta)$ i.e., for any $\varepsilon > 0$, we construct an (n, n)-code

(F, g) such that:

$$\mathbb{E}\big[d\big(A^n, g(B^n, Y^n)\big)\big] \leq D + \varepsilon \,,$$
$$\frac{1}{n} H(A^n|E^n Z^n) \geq \Delta - \varepsilon \,.$$

In this scheme, Alice compresses the source A in descriptions (U, V), with V on the top of U. Digital random noise r_f is also transmitted on V (a la Gelfand-Pinsker) to take advantage of the possibly better quality of Bob's channel, and prevent Eve from decoding the whole message. As in the classical wiretap channel [32, 90], its rate R_f satisfies some constraint that allows to characterize the equivocation rate at Eve. Alice finally sends some deterministic function $x(V, A)$ of V and A.

Let $\varepsilon > 0$, $R_1, R_2, R_f \in \mathbb{R}_+^*$ such that

$$R_2 + R_f < I(V; AZ|U) \,, \tag{3.20}$$

and assume that a local (independent and uniformly distributed) random source with rate R_f is available at Alice. Define $\gamma = \frac{\varepsilon}{7\, d_{\max}}$.

3.7.1 Codebook generation

Randomly pick 2^{nR_1} sequences $u^n(r_1)$ from $T_\delta^n(U)$. Then, for each codeword $u^n(r_1)$, randomly pick $2^{n(R_2+R_f)}$ sequences $v^n(r_1, r_2, r_f)$ from $T_\delta^n(V|u^n(r_1))$. See Figure 3.10.

3.7.2 Encoding procedure

Assume that source sequence A^n and random noise r_f are produced at Alice.

Look for the first codeword $u^n(r_1)$ such that $(u^n(r_1), A^n) \in T_\delta^n(U, A)$. Then look for the first codeword $v^n(r_1, r_2, r_f)$ such that $(v^n(r_1, r_2, r_f), A^n) \in T_\delta^n(V, A|u^n(r_1))$.

Alice then sends $X^n = F(A^n)$ defined by the following component-wise relation, for each $i = \{1, \ldots, n\}$:

$$X_i \triangleq x(v_i(r_1, r_2, r_f), A_i) \,.$$

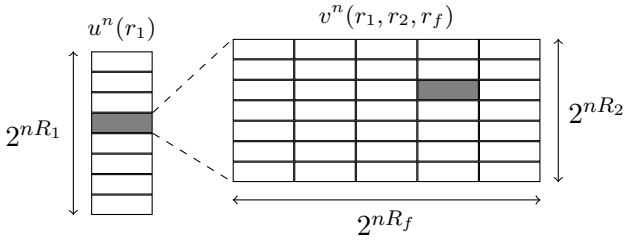


Figure 3.10: Hybrid scheme–Codebook.

3.7.3 Decoding procedure

Assume that Bob observes B^n and receives Y^n from Alice.

Look for the unique codeword $u^n(r_1)$ such that $(u^n(r_1), B^n, Y^n) \in T_\delta^n(U, B, Y)$. Then look for the unique $v^n(r_1, r_2, r_f)$ such that $(v^n(r_1, r_2, r_f), B^n, Y^n) \in T_\delta^n(V, B, Y|u^n(r_1))$.

Compute the estimate $g(B^n, Y^n) \in \mathcal{A}^n$ using the following component-wise relation, for each $i = \{1, \ldots, n\}$:

$$g_i(B^n, Y^n) \triangleq \hat{A}(v_i(r_1, r_2, r_f), B_i, Y_i) \, .$$

3.7.4 Errors and constraints

Denoting by E the event "An error occurred during the encoding or decoding steps," we expand its probability (averaged over the set of all possible codebooks) as follows: $\Pr\{\mathsf{E}\} \leq P_{t,1} + P_{t,2} + P_{e,1} + P_{e,2} + P_{d,1} + P_{d,2}$, where each term corresponds to a particular error event, as detailed below. We derive sufficient conditions on the parameters that make each of these probabilities small.

3.7.4.1 Typicality

From standard properties of typical sequences (see Appendix A), there exists a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that $P_{t,1} \triangleq \Pr\{(A^n, B^n, E^n) \notin T_\delta^n(A, B, E)\} \leq \eta_n$. Consequently, $P_{t,1} \leq \gamma$ for some sufficiently large n.

Similarly, since the input of the channel X^n is typical (when no error occurs during the encoding steps), $P_{t,2} \triangleq \Pr\{(X^n, Y^n, Z^n) \notin T_\delta^n(X, Y, Z)\} \leq \gamma$ for some sufficiently large n.

3.7.4.2 Encoding

In the first encoding step, Alice needs to find (at least) one codeword $u^n(r_1)$ such that $(u^n(r_1), A^n) \in T_\delta^n(U, A)$. Following the argument of Section 2.3.4.2, we can prove that if $R_1 > I(U; A)$, then the probability that this step fails $P_{e,1}$ can be upper bounded by γ for some sufficiently large n.

Similarly, the second encoding step succeeds with probability $1 - P_{e,2} \geq 1 - \gamma$ under condition $R_2 > I(V; A|U)$.

3.7.4.3 Decoding

In the first decoding step, Alice should find the unique codeword $u^n(r_1)$ such that $(u^n(r_1), B^n, Y^n) \in T_\delta^n(U, B, Y)$. The corresponding error probability $P_{d,1}$ must be carefully handled.

As previously noted in [84,91], the conventional random coding proof technique does not apply here. In the proposed joint coding scheme, a single codebook plays both roles of source and channel codebooks. For a given source sequence a^n, the indices (r_1, r_2) thus

depend on the entire codebooks, and the averaging over the set of all possible codebooks cannot be performed in the usual way. Similarly to [91], we can prove the following lemma.

Lemma 3.9. *There exists $\kappa < 1$ and a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that*

$$P_{d,1} \leq \frac{2^{n(R_1 - I(U;BY)+\eta_n)}}{(1-\kappa)^2} ,$$

for some sufficiently large n.

Proof. See Appendix E.3. □

From Lemma 3.9, if $R_1 < I(U;BY)$, then probability $P_{d,1}$ vanishes as n tends to infinity, and hence can be upper bounded by γ for some sufficiently large n.

Using similar arguments, we can prove that the second decoding step succeeds with probability $1 - P_{d,2} \geq 1 - \gamma$ under condition $R_2 + R_f < I(V;BY|U)$.

3.7.4.4 Summary

In this paragraph, we proved that under some sufficient conditions, $\Pr\{\mathsf{E}\} \leq 6\gamma$.

3.7.5 Distortion at Bob

We now check that our code achieves the required distortion level at Bob (averaged over the set of all possible codebooks):

$$\begin{aligned}\mathbb{E}\Big[d\big(A^n, g(B^n, Y^n)\big)\Big] &\leq (1 - \Pr\{\mathsf{E}\})\mathbb{E}\left[d\big(A^n, \hat{A}\big(v^n(r_1, r_2, r_f), B^n, Y^n\big)\big)\middle|\not{\mathsf{E}}\right] + \Pr\{\mathsf{E}\}\, d_{\max} \\ &\leq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] + \frac{\varepsilon}{7} + \frac{6\varepsilon}{7} ,\end{aligned}$$

where the last inequality holds for some sufficiently large n, and follows from $\Pr\{\mathsf{E}\} \leq 6\gamma$, the definition of γ, and the argument given in Section 2.3.5.

Condition $D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big]$ is thus sufficient to achieve distortion $D + \varepsilon$.

3.7.6 Equivocation rate at Eve

The equivocation at Eve can be divided in "source" and "channel" terms. Each one is studied using standard properties of typical sequences, and following the arguments of

Section 2.3.6 and [90, Section 2.3.*Step 3*]:

$$\begin{aligned}
H(A^n|E^nZ^n) &= H(r_1r_2r_fA^nX^n|E^nZ^n) - H(r_1r_2r_fX^n|A^nE^nZ^n) \\
&\overset{(a)}{=} H(r_1r_2r_fA^nX^n|E^nZ^n) - H(r_2r_f|r_1A^nZ^n) \\
&\overset{(b)}{\geq} H(r_1r_2r_fA^nX^n|E^nZ^n) - n\,\tfrac{\varepsilon}{4} \\
&\overset{(c)}{\geq} H(r_2r_fA^nX^n|r_1E^nZ^n) - n\,\tfrac{\varepsilon}{4} \\
&= H(r_2r_fA^nX^n|r_1) + H(E^nZ^n|r_1r_2r_fA^nX^n) - H(E^nZ^n|r_1) - n\,\tfrac{\varepsilon}{4} \\
&\overset{(d)}{=} H(r_fA^n|r_1) + H(E^nZ^n|A^nX^n) - H(E^nZ^n|r_1) - n\,\tfrac{\varepsilon}{4} \\
&\overset{(e)}{=} H(A^n|r_1) + H(r_f) + H(E^n|A^n) + H(Z^n|X^n) \\
&\qquad\qquad - H(E^nZ^n|r_1) - n\,\tfrac{\varepsilon}{4}\ , \qquad (3.21)
\end{aligned}$$

where

- step (a) follows from the fact that X^n (resp. r_1) is a deterministic function of (r_1, r_2, r_f, A^n) (resp. A^n), and the Markov chain $(r_2, r_f) \multimap (A^n, Z^n) \multimap E^n$,
- step (b) from condition (3.20) (which ensures that Eve can decode $v^n(r_1, r_2, r_f)$ from $(u^n(r_1), A^n, Z^n)$ with an arbitrarily small probability of error, using a decoder similar to Bob's one–see Sections 3.7.3, 3.7.4), and Fano's inequality (for some sufficiently large n),
- step (c) from the fact that conditioning reduces the entropy,
- step (d) from the fact that (r_2, X^n) is a deterministic function of (r_1, r_f, A^n), and the Markov chain $(E^n, Z^n) \multimap (A^n, X^n) \multimap (r_1, r_2, r_f)$,
- step (e) from the fact that r_f is independent of (r_1, A^n), and the Markov chains $E^n \multimap A^n \multimap (X^n, Z^n)$, $Z^n \multimap X^n \multimap (A^n, E^n)$.

We now separately study each term of the r.h.s. of (3.21):

- From the fact that the codewords $u^n(r_1)$ are drawn i.i.d., and following the argument of Lemma 2.5, we can prove that

$$H(A^n|r_1) \geq n\left(H(A|U) - \tfrac{\varepsilon}{4}\right)\ ,$$

  for some sufficiently large n.

- Since the random source r_f is uniformly distributed with rate R_f:

$$H(r_f) = nR_f\ .$$

- Since the sources are i.i.d.:

$$H(E^n|A^n) = nH(E|A)\ .$$

- Since the channel is memoryless and the input X^n is typical (see [90, Eq. (2.46)]),

$$H(Z^n|X^n) \geq n\left(H(Z|X) - \tfrac{\varepsilon}{4}\right) .$$

- From the fact that $(u^n(r_1), E^n, Z^n)$ are jointly typical, and following the arguments of [90, Eq. (2.54)], we can prove that

$$H(E^n Z^n|r_1) \leq n\left(H(EZ|U) + \tfrac{\varepsilon}{4}\right) .$$

Gathering all the above equations, we proved that

$$H(A^n|E^n Z^n) \geq n\Big(H(A|U) + R_f + H(E|A) + H(Z|X) - H(EZ|U) - \varepsilon\Big) ,$$

for some sufficiently large n.

After some algebraic manipulations using the Markov chains $U \multimap A \multimap E$ and $(U, E) \multimap X \multimap Z$, we proved that the following condition is sufficient to achieve equivocation rate $\Delta - \varepsilon$ at Eve:

$$\Delta \leq H(A|UE) - I(X; Z|UE) + R_f .$$

3.7.7 End of proof

In this section, we proved that sufficient conditions for the achievability of a tuple $(k = 1, D, \Delta)$ are given by the following system of inequalities:

$$\begin{cases} R_1 > I(U; A) \\ R_2 > I(V; A|U) \\ R_f > 0 \\ R_1 < I(U; BY) \\ R_2 + R_f < I(V; BY|U) \\ R_2 + R_f < I(V; AZ|U) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] \\ \Delta \leq H(A|UE) - I(X; Z|UE) + R_f \end{cases}$$

Fourier-Motzkin elimination [156] then yields:

$$\begin{cases} I(U; A) < I(U; BY) \\ I(V; A|U) < I(V; BY|U) \\ D \geq \mathbb{E}\big[d(A, \hat{A}(V, B, Y))\big] \\ \Delta < H(A|UE) - I(X; Z|UE) + I(V; BY|U) - I(V; A|U) \\ \Delta < H(A|UE) - I(X; Z|UE) + I(V; AZ|U) - I(V; A|U) \end{cases}$$

This proves Theorem 3.8. □

3.8 Secure transmission of a binary source with BEC/BSC side informations over a type-II wiretap channel (continued)

In this section, we go back on the binary example introduced in Section 3.5 and compare a hybrid coding scheme based on Theorem 3.8 with the ones analyzed is Section 3.5, namely the digital scheme of Section 3.3 (see Proposition 3.6) and a pure analog one consisting in directly sending the source over the channel (see Proposition 3.7).

3.8.1 Hybrid coding

We consider the hybrid scheme of Theorem 3.8 choosing variables U, V and X as follows:

$$U = V \oplus W \,, \tag{3.22}$$

$$V \overset{\perp\!\!\!\perp A}{\sim} \mathcal{B}(\tfrac{1}{2}) \,, \tag{3.23}$$

$$X = V \oplus A \,, \tag{3.24}$$

where $\oplus$ stands for the binary exclusive-or operator, W is independent of A and V, and $W \sim \mathcal{B}(u)$ for some crossover probability $u \in [0, \frac{1}{2}]$.

3.8.2 Numerical results

Figure 3.11 represents the largest equivocation rate at Eve Δ as a function of the erasure probability β for

(*i*) the outer bound of Proposition 3.5,

(*ii*) the hybrid digital/analog scheme of Theorem 3.8 with variables (3.22)–(3.24) (and optimizing over u),

(*iii*) the digital scheme of Proposition 3.6 (optimizing over u and q),

(*iv*) the analog scheme of Proposition 3.7,

for parameter values $\epsilon = 0.1$, $\zeta = 0.1$.

If $\beta \leq 4\epsilon(1-\epsilon)$, B is less noisy than E (see Figure 3.8), and the digital scheme is optimal (as stated by Proposition 3.3), as well as the proposed hybrid one. Here, this result also seems to hold when B is only more capable than E i.e., for $\beta \leq h_2(\epsilon)$.

For $\beta = 1$, as already noted in Section 3.5.3, the naive pure analog scheme outperforms the digital one. According to the comments of Section 3.6.2.1, the proposed hybrid digital/analog scheme always performs as good as the analog one.

In Figure 3.11, the proposed hybrid digital/analog scheme also seems to perform as good as the digital one. However, according to the comments of Section 3.6.2.2, and depending on the parameters ϵ, ζ, this may not be the case for all values β in $[h_2(\epsilon), 1)$.

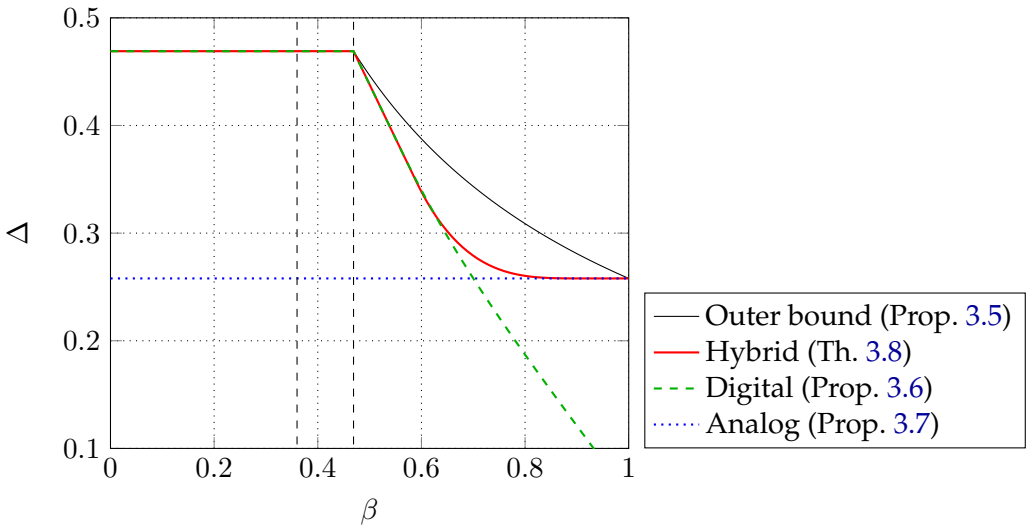


Figure 3.11: Equivocation rate Δ as a function of erasure probability β ($\epsilon = 0.1$, $\zeta = 0.1$).

3.9 Secure transmission of a Gaussian source over a Gaussian wiretap channel

3.9.1 System model

In this section, we consider the transmission of a Gaussian source over a Gaussian wiretap channel with matched bandwidth. More precisely, as depicted in Figure 3.12, the source at Alice A is standard Gaussian, and observations at Bob and Eve are the outputs of independent additive white Gaussian noise (AWGN) channels with input A and respective noise powers P_B and P_E. Communication channels from Alice to Bob and Eve are AWGN channels with respective noise powers P_Y and P_Z. The average input power of this channel is limited to P. One channel use is allowed per source symbol.

Euclidean distance on $\mathbb{R}$ is used to measure distortion at Bob ($d(a,b) = (a-b)^2$, for each $a, b \in \mathbb{R}$). Differential entropy $h(\cdot)$ measures uncertainty yielding equivocation rates $\Delta \in \mathbb{R}$. We also introduce quantity $D_E = 2^{2\Delta}/(2\pi e)$, which provides a lower bound on the minimum mean-square error of any estimator of A at Eve [31, Theorem 8.6.6].

Definition 3.3 (Achievability)**.** In this section, a tuple $(D, D_E) \in {\mathbb{R}_+^*}^2$ is said to be *achievable* if, for any $\varepsilon > 0$, there exists an (n,n)-code (F,g) such that:

$$\begin{aligned} \mathbb{E}\big[\,\|A^n - g(B^n, Y^n)\|^2\,\big] &\leq D + \varepsilon\,, \\ \frac{1}{n}\,h(A^n|E^n Z^n) &\geq \frac{1}{2}\log\left(2\pi e\, D_E\right) - \varepsilon\,, \\ \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\big[X_i^2\big] &\leq P + \varepsilon\,, \end{aligned}$$

with channel input X^n as the output of the encoder $F(A^n)$.

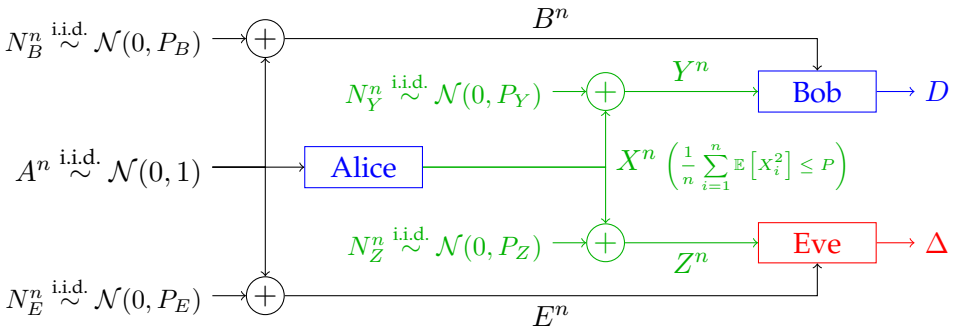


Figure 3.12: Transmission of a Gaussian source over a Gaussian wiretap channel with side information.

Although Theorems 3.1, 3.2, 3.8 are stated and proved for finite alphabets, we take the liberty to use their statements as inner/outer regions also for this quadratic Gaussian case. The involved probability distributions should now also verify condition

$$\text{Var}\left[X\right] \leq P \,. \tag{3.25}$$

The corresponding regions will be denoted with an additional $\cdot^P$ i.e., $\mathcal{R}_{\text{out}}^P$, $\mathcal{R}_{\text{digital}}^P$ and $\mathcal{R}_{\text{hybrid}}^P$.

Notice that due to the Gaussian additive noises, and depending on the relative values of P_B, P_E (resp. P_Y, P_Z), one side information (resp. one channel) is a stochastically degraded version of the other. There exist four different cases and from the results of Section 3.3.3 separation holds for three of them, as summarized in Table 3.1. As a matter of fact, the case when Bob has "better" channel ($P_Y < P_Z$) and "worse" side information ($P_B > P_E$) than Eve is still open. We next propose a hybrid digital/analog scheme based on Theorem 3.8 that turns out to be optimal when $P_Y < P_Z$ and $P_B \to \infty$.

3.9.2 Hybrid coding

Proposition 3.10 below follows from Theorem 3.8 choosing variables U, V and X as follows:

$$U = \emptyset \,, \tag{3.26}$$

$$V = \alpha A + \gamma N \,, \tag{3.27}$$

$$X = \big(\beta A - \gamma N\big)\sqrt{P} \,, \tag{3.28}$$

where $\alpha \in \mathbb{R}$, $\beta \in [0,1)$, $\gamma = \sqrt{1-\beta^2}$ and $N \sim \mathcal{N}(0,1)$ is a standard Gaussian random variable independent of A. Note that $X \sim \mathcal{N}(0,P)$ writes as a deterministic function of A and V:

$$X = \big((\alpha+\beta)A - V\big)\sqrt{P} \,. \tag{3.29}$$

Function $\hat{A}$ is defined as the MMSE estimator of A from (V, B, Y).

	$P_B \leq P_E$	$P_B > P_E$
$P_Y < P_Z$	✓	?
$P_Y \geq P_Z$	✓	✓

Table 3.1: Cases where $\mathcal{R}_{\text{digital}}$ is tight and separation holds.

The hybrid digital/analog scheme of Section 3.6 with variables (3.26)–(3.28) reduces to the one depicted in Figure 3.13.

Proposition 3.10 (Hybrid scheme). *A tuple* $(D, D_E) \in {\mathbb{R}_+^*}^2$ *is achievable if*

$$D \geq \frac{1}{1 + \frac{1}{P_B} + \frac{\alpha^2}{\gamma^2} + \frac{P}{P_Y}(\alpha+\beta)^2} , \tag{3.30}$$

$$D_E \leq \frac{1}{1 + \frac{1}{P_E} + \frac{P}{P_Z}\left(1 + \frac{\gamma^2}{P_E}\right)} \cdot \min\left\{ \frac{1 + \frac{1}{P_B} + \frac{P}{P_Y}\left(1 + \frac{\gamma^2}{P_B}\right)}{1 + \frac{1}{P_B} + \frac{\alpha^2}{\gamma^2} + \frac{P}{P_Y}(\alpha+\beta)^2} ; 1 + \gamma^2 \frac{P}{P_Z} \right\} , \tag{3.31}$$

for some $\alpha \in \mathbb{R}$, $\beta \in [0, 1)$ *such that*

$$\frac{\alpha^2}{\gamma^2} + \frac{P}{P_Y}(\alpha+\beta)^2 \leq \frac{P}{P_Y}\left(1 + \frac{\gamma^2}{P_B}\right) , \tag{3.32}$$

where

$$\gamma = \sqrt{1 - \beta^2} . \tag{3.33}$$

Proof. See Appendix E.4. □

Remark 3.3. In the proposed scheme, unlike dirty-paper coding for point-to-point communication without secrecy constraint [30], the source A (that can be viewed as the state of some channel, known at the encoder –see Figure 3.9) and the channel input X are not independent.

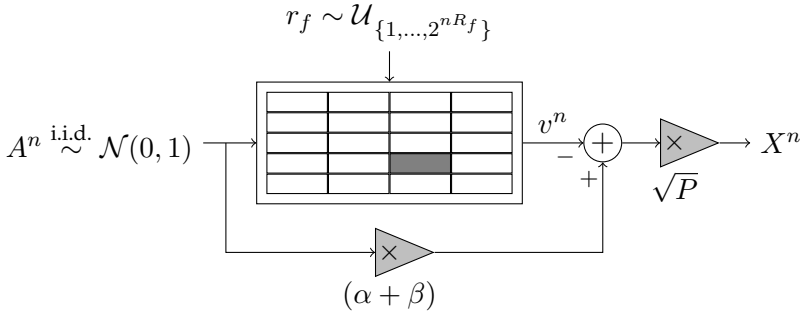


Figure 3.13: Hybrid digital/analog scheme for secure transmission of a Gaussian source over a Gaussian wiretap channel.

3.9.3 Special case: $P_Y < P_Z$, $P_B \to \infty$

From now on, we focus on the unsolved case (represented by "?" in Table 3.1). In particular, we assume that $P_Y < P_Z$. Then, if Bob does not have any side information i.e., $B = \emptyset$ or equivalently $P_B \to \infty$:

- The hybrid digital/analog scheme of Proposition 3.10 is optimal and yields Theorem 3.11.
- The digital scheme of Theorem 3.2 is strictly sub-optimal, as shown by Proposition 3.12 and Figure 3.14.

Theorem 3.11 (Optimal characterization). *If $P_Y < P_Z$ and $B = \emptyset$, $(D, D_E) \in {\mathbb{R}_+^*}^2$ is achievable if and only if*

$$D \geq \frac{1}{1+\frac{P}{P_Y}}\,, \tag{3.34}$$

$$D_E \leq \frac{1}{\max\left\{1\,;\,\frac{1}{D}\cdot\frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}\right\}+\frac{1}{P_E}}\,. \tag{3.35}$$

Proof. The proof of the converse part is given in Appendix E.5.

The direct part follows after Proposition 3.10 by letting P_B tend to infinity and choosing, for any distortion level $D \in \left[\frac{1}{1+\frac{P}{P_Y}}, \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}\right)$:

$$\alpha = \frac{\beta + \gamma^2\sqrt{\frac{1}{D}\left(\frac{P}{P_Y}-\frac{P}{P_Z}\right)}}{1+\gamma^2\frac{P}{P_Y}} - \beta\,, \tag{3.36}$$

$$\beta = \sqrt{\frac{P_Z}{P}}\sqrt{1+\frac{P}{P_Z}-D\left(1+\frac{P}{P_Y}\right)}\,. \tag{3.37}$$

Details are provided in Appendix E.6. □

The following proposition provides a simple expression of region $\mathcal{R}^P_{\text{digital}}$ i.e., the set of all tuples achievable by the digital scheme of Section 3.3.

Proposition 3.12 (Digital scheme). *If $P_Y < P_Z$ and $B = \emptyset$, $(D, D_E) \in \mathcal{R}^P_{digital}$ if and only if*

$$D \geq \frac{1}{1+\frac{P}{P_Y}}\,, \tag{3.38}$$

$$D_E \leq \frac{1}{\frac{1}{\mu}+\frac{1}{P_E}}\cdot\min\left\{1\,;\,\frac{D\left(1+\frac{P}{P_Y}\right)}{1+\mu\frac{P}{P_Z}-(1-\mu)\frac{P_Y}{P_Z}}\right\}\,, \tag{3.39}$$

for some $\mu \in \left[\frac{1}{1+\frac{P}{P_Y}}, 1\right]$.

Proof. The proof of the converse part is similar to the one of Theorem 3.11 and is given in Appendix E.7.

The direct part follows from Theorem 3.2 with Gaussian variables U, V, Q and $T = X$ after some straightforward derivations. Details are omitted. □

Remark 3.4. If $D \geq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$, then $\mu = 1$ is optimal in Proposition 3.12, yielding inequalities (3.34), (3.35) in Theorem 3.11. This implies that the digital scheme of Section 3.3 is optimal in this region. For such distortion levels, the quantity $D_E = \frac{1}{1+\frac{1}{P_E}} = \mathrm{Var}\,[A|E]$ is achievable, meaning that Eve cannot retrieve additional information from the communication between Alice and Bob.

In the following, we will also compare the two above schemes with a pure analog one, consisting in directly sending a scaled version of the source over the channel. Its performance is given by the following proposition.

Proposition 3.13 (Analog scheme)**.** *If $B = \emptyset$, $(D, D_E) \in {\mathbb{R}_+^*}^2$ is achievable through an analog scheme if*

$$D \geq \frac{1}{1+\frac{P}{P_Y}},$$
$$D_E \leq \frac{1}{1+\frac{1}{P_E}+\left[\left(\frac{1}{D}-1\right)\frac{P_Y}{P_Z}\right]_+}.$$

Proof. See Appendix E.8. □

Remark 3.5. If $D = D_{\min} \triangleq \frac{1}{1+\frac{P}{P_Y}}$, then Proposition 3.13 yields inequalities (3.34), (3.35) in Theorem 3.11 i.e., the above analog scheme is optimal.

Remark 3.6. When there is no secrecy requirement i.e., $D_E = 0$, all the above schemes can achieve distortion $D_{\min}$, as stated in [47, 52].

Numerical results

Figure 3.14 represents the largest achievable D_E as a function of the distortion level at Bob D for

(*i*) the optimal hybrid digital/analog scheme of Theorem 3.11,

(*ii*) the digital scheme of Proposition 3.12 (optimizing over μ),

(*iii*) the analog scheme of Proposition 3.13,

for parameter values $P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$.

As a matter of fact, the proposed hybrid digital/analog scheme outperforms both pure analog and digital schemes. Furthermore, while the digital scheme is optimal for

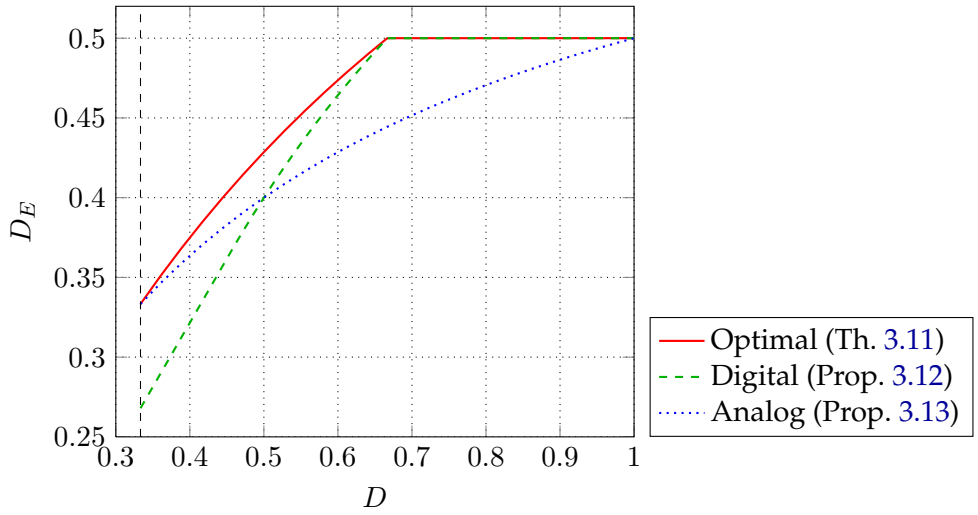


Figure 3.14: Quantity D_E as a function of the distortion at Bob D ($P = 1$, $P_Y = 0.5$, $P_Z = 1$, $P_E = 1$).

$D \geq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$ (Remark 3.4) and the analog one for $D = D_{\min}$ (Remark 3.5), a time-sharing combination of these falls short to achieve the entire region, as shown by Figure 3.14 and Theorem 3.11.

Remark 3.7. While the hybrid digital/analog scheme of Section 3.9.2 can be used regardless of the values of the parameters, we did not manage to prove a result of optimality in the more general case where $P_B < \infty$. As a matter of fact, the argument used in both the converse part of Theorem 3.11 and Proposition 3.12 fails (e.g., the EPI does not directly apply to the quantities of interest). We then were not able to maximize neither the outer bound of Theorem 3.1, nor the inner bound of Theorem 3.2, so that there is no region to compare Proposition 3.10 with.

3.10 Summary

In this chapter, we have investigated the general problem of source-channel coding for secure transmission of sources over noisy channels with side information at the receivers. This setting can be seen as a generalization of the problems of secure source coding with side information at the decoders (investigated in Section 2.4), and the wiretap channel. A general outer bound on the corresponding achievable region has been derived, as well as two inner bounds based on (*i*) a pure digital scheme which combines secure source coding of Chapter 2 with coding for broadcast channels with confidential messages [32], and (*ii*) a novel hybrid digital/analog scheme (in the matched-bandwidth case).

The proposed bounds do not match in general, but the digital scheme turns out to be optimal under some less noisy conditions. However, a simple counterexample shows

that a *joint* source-channel scheme may achieve better performance in some other cases. At first look, this is not surprising since it is well-known that *joint* source-channel coding/decoding are well-suited for broadcast channels without secrecy constraints [155], when all decoders must perfectly reconstruct the source. But the *secure* setting is rather different because Alice only wants to help one receiver (Bob), while she wants to blur the other one (Eve). Therefore, the intuition indicates that the optimal strategy would be the opposite i.e., separation between source and channel encoders, as in Propositions 3.3 and 3.4.

On the other hand, the proposed hybrid digital/analog scheme can be useful in terms of secrecy. In a quadratic Gaussian setup when side information is only present at the eavesdropper, this strategy turns out to be optimal. In a more general case where both receivers have side information, the entropy power inequality fails but the I-MMSE relation [58], which has already been proved useful in many point-to-point [100, 124] and multiterminal settings [39, 59], may yield the expected converse.

CHAPTER 4

High-Rate Vector Quantization for the Neyman-Pearson Detection of Correlated Processes

Abstract. In this chapter, the effect of quantization on the performance of the Neyman-Pearson test is investigated. It is assumed that a sensing unit observes samples of a correlated stationary ergodic multivariate process. Each sample is passed through an N-point quantizer and transmitted to a decision device which performs a binary hypothesis test. For any false alarm level, it is shown that the miss probability of the Neyman-Pearson test converges to zero exponentially as the number of samples tends to infinity, assuming that the observed process satisfies certain mixing conditions. The main contribution of this chapter is to provide a compact closed-form expression of the error exponent in the high-rate regime i.e., when the number N of quantization levels tends to infinity, generalizing previous results of Gupta and Hero to the case of non-independent observations. If d represents the dimension of one sample, it is proved that the error exponent converges at rate $N^{2/d}$ to the one obtained in the absence of quantization. As an application, relevant high-rate quantization strategies which lead to a large error exponent are determined. Numerical results indicate that the proposed quantization rule can yield better performance than existing ones in terms of detection error.

4.1 Introduction

Consider a sensing unit which transmits a sequence of measurements to a decision device (DD) whose mission is to detect a given signal. For example, a CCTV camera in a surveillance system transmits its data to a remote controller interested in the detection of a particular object in its field of view. This situation also arises in the context of wireless sensor networks (WSN) where a fusion center collects the individual measurements of a large number of identical sensors and processes these measurements in order to detect abnormal events [5, 25]. In such applications, due to bandwidth, delay or storage limitations, transmitted data rates are often limited. Therefore, measurements must be quantized prior to transmission. As a matter of fact, this quantization step may severely degrade the overall detection performance of the system. In this chapter, we consider that a binary hypothesis test is performed at the DD. The available data set corresponds to a quantized version of a stationary ergodic discrete-time multivariate process. Our aim is

to quantify the detection performance of a given quantizer and characterize quantization strategies which guarantee attractive performance at the DD.

In the past decades, numerous papers were dedicated to the search for relevant quantization strategies and their practical design [54]. The most popular criterion used to select quantizers is the mean square error (MSE) between the quantized signal and the initial source [50]. An analytical characterization of quantizers minimizing the MSE is difficult in the general case. Bennett [8] pioneered the study of *high-rate* (or *high-resolution*) quantization for the reconstruction of scalar signals. The idea of Bennett was to study the MSE in the asymptotic regime where the number of quantization levels tends to infinity. A closed-form expression of the (properly normalized) MSE can be determined in that case, and the families of quantizers minimizing the asymptotic MSE can be directly characterized. Extension of the work of Bennett to vector-valued observations was later achieved in [111]. However, the MSE criterion is especially relevant when the aim is to reconstruct the source. On the other hand, it can be inappropriate as far as other applications are concerned. For this reason, various distortion measures have been proposed in the literature in a *task-oriented* setting for estimation [108, 129, 167], detection [61, 74, 128, 130, 149, 153, 154], and classification [125] (see also [64]). In particular, considerable attention has been paid to optimal quantization for hypothesis testing. Poor and Thomas [130] used Ali-Silvey distances between densities. Later, Poor [129] proposed the generalized f-divergence and studied this distortion measure in the high-rate regime. Picinbono and Duvaut [128] considered a deflection criterion and proved that the corresponding optimal procedure corresponds to the scalar quantization of the likelihood ratio. Tsitsiklis [154] studied the properties of such quantizers with respect to several distortion measures. More recently, following the initial works of Tenney and Sandell [149], Tsitsiklis [153], and Benitz and Bucklew [7], Gupta and Hero [61] investigated the selection of high-rate quantizers for binary hypothesis tests. In their setting, the decision device gathers a sequence of n independent and identically distributed (i.i.d.) variables, each of these variables being passed through a fixed quantizer. The probability density function (p.d.f.) of the samples is assumed to be known both under the null hypothesis and the alternative. In this case, it is well known that a uniformly most powerful test is obtained by the Neyman-Pearson (NP) procedure which consists in rejecting the null hypothesis when the log-likelihood ratio (LLR) exceeds a certain threshold [87]. The threshold is usually chosen in such a way that the probability of false alarm of the test (that is, the probability to decide the alternative under the null hypothesis) is fixed to a specified *level*, say α. The performance of the NP test of level α can be evaluated in terms of the miss probability (that is, the probability to decide the null hypothesis under the alternative). In our case, the miss probability clearly depends on the quantizer used by the sensing unit. Thus, a natural approach would be to select the quantizer which minimizes the miss probability. Unfortunately, the miss probability does not admit any tractable expression as a function of the quantizer. To circumvent this issue, it is convenient to study the miss probability in the case where the number n of available snapshots tends to infinity. In case of i.i.d. observations, the celebrated Stein's lemma [31] states that the miss

probability tends to zero exponentially in n. Based on this result, it is relevant to select the quantizers which yield a large value of the error exponent. Unfortunately, the maximization of the error exponent as a function of the quantizer is impractical. Following the idea of [8,111], Gupta and Hero restricted their attention to high-rate quantizers and managed to obtain a compact expression of the error exponent loss induced by quantization.

Most of this work addresses the case where observations are independent random variables. However, the detection of a correlated process is a crucial issue in many applications [24, 62, 144, 160]. In this case, fewer results are available in the literature. Chamberland and Veeravalli [24] analyzed the impact of the density of sensors in a WSN on the detection performance, when observations are correlated. Willett et al. [160] studied the one-bit quantization of a pair of dependent Gaussian random variables. In case of the detection of a Gauss-Markov signal in noise, Sung et al. [144] proved that for a fixed false alarm level, the miss probability of the NP test converges exponentially to zero, and provided a closed-form expression of the error exponent. Hachem et al. [62] later extended the results of [144] to irregularly sampled Gaussian diffusion processes. However, [62, 144] assume that the DD has a perfect access to the observations of the sensing unit, and do not address quantization issues.

In this chapter, we study the performance of the Neyman-Pearson test based on a quantized version of a stationary ergodic multivariate process. We generalize the work of Gupta and Hero [61] to the case where the observed process is non-i.i.d. (either under the null hypothesis, the alternative, or both). In this situation, Stein's lemma does not directly apply. The error exponent does no longer admit a closed-form expression and the determination of relevant quantizers is therefore a more difficult task. Provided that the process of interest satisfies certain forgetting properties (present observations should become nearly independent of past observations after a sufficient amount of time), we prove that the miss probability of the NP test of level α tends exponentially to zero as the number of observations tends to infinity. Our main contribution is to provide a compact closed-form expression of the error exponent in case of high-rate quantizers. If N denotes the number of quantization levels (or equivalently if each measurement is quantized on $\log_2(N)$ bits), we prove that the error exponent achieved when using quantized observations converges as N tends to infinity to the ideal error exponent that one would obtain if perfect/unquantized measurements were available at the DD. More precisely, we prove that the error exponent loss tends to zero at speed $N^{-2/d}$ where d represents the dimension of each individual measurement. The asymptotic error exponent depends on the process distributions under both hypotheses. It also depends on the quantization strategy through the so-called *model point density* and *model covariation profile*. The model point density can be interpreted as the asymptotic density of cells in the neighborhood of each point of the observation space. The model covariation profile captures the shape of the cells. As a consequence, the selection of relevant high-rate quantizers reduces to the determination of the point densities and covariation profiles minimizing the asymptotic error exponent loss. In case of scalar quantization ($d = 1$), our compact expression immediately yields a simple characterization of optimal high-rate quantizers.

In case of vector quantization ($d \geq 2$), an exact characterization of optimal quantizers is more difficult. Following the approach of [61] once again, we nevertheless determine relevant families of quantizers with attractive error exponent. Note that our theoretical results hold under the assumption that the observed process "forgets" past observations fast enough. As a special case, we prove that our assumptions hold for a general class of hidden Markov models verifying a certain contraction property. Numerical illustrations are provided in the case where the measurements correspond to a modulated signal in the In-phase/Quadrature plane.

The rest of this chapter is organized as follows. In Section 4.2, we describe the observation model. We also review some known results on Neyman-Pearson tests, and derive the associated error exponent in the ideal case where the DD has perfect access to the measurements. The vector quantization framework is introduced in Section 4.3. In Section 4.4, the impact of quantization on the error exponent is evaluated in the high-rate regime. We determine relevant quantization strategies allowing to reduce this degradation. Section 4.5 is devoted to the proof of the main result. In Section 4.6, we illustrate our findings in the special case of hidden Markov processes and give sufficient conditions on the transition and observation kernels ensuring that our results apply. Section 4.7 is dedicated to numerical illustrations. Finally, Section 4.8 concludes the chapter.

Notation

For any sequence $(y_i)_{i\in\mathbb{Z}}$, for any integers $k \leq \ell$, notation $y_{k:\ell}$ stands for the collection $(y_k, y_{k+1}, \ldots, y_\ell)$ and notation $y_{\mathbb{Z}}$ is used to designate the whole sequence. If y is a vector with dimension d, we denote by $y^{(i)}$ its i-th component and $\|y\|$ its Euclidean norm. We denote by $\|A\|$ the spectral norm of any square matrix A. Notation $.^{\mathrm{T}}$ stands for the transpose operator.

A real-valued function $f\colon y_{k:\ell} \mapsto f(y_{k:\ell})$ on $\mathsf{S} \subset \mathbb{R}^d \times \cdots \times \mathbb{R}^d$ is said to be of class C_3 on S if it is three times continuously differentiable on S. We denote by $\nabla_{y_m} f(y_{k:\ell})$ its gradient w.r.t. y_m at point $y_{k:\ell}$. When no variable is specified, $\nabla g(y)$ simply denotes the (d-dimensional) gradient of the real-valued single-variable function $y \mapsto g(y)$ defined on $\mathsf{Y} \subset \mathbb{R}^d$. We define the Hessian matrix of f by $\left[\nabla^2_{y_m,y_n} f\right]_{i,j} = \frac{\partial^2 f}{\partial y_m^{(i)}\, \partial y_n^{(j)}}$ for all $i, j \in \{1, \ldots, d\}$. Moreover, notation $\nabla^2_{y_m}$ stands for $\nabla^2_{y_m,y_m}$.

Notation $B(\mathsf{X})$ stands for the Borel σ-field on X. Notation $\sigma(Y_{1:n})$ stands for the sub-σ-field of $B(\mathsf{Y}^{\mathbb{Z}})$, associated with the random vector $Y_{1:n}$. Notation $\xrightarrow[n\to\infty]{P}$ stands for the convergence in probability as $n \to \infty$. Notation $\xrightarrow[n\to\infty]{L^r(\mathbb{P}_0)}$ stands for the convergence in the L^r-norm w.r.t. probability $\mathbb{P}_0$.

The natural logarithm is denoted by $\log(\cdot)$. Notation $\circ$ stands for the composition operator i.e., for any arbitrary functions f and g, $f \circ g(x) = f(g(x))$. Notation $o_N(\cdot)$ is a little-o notation as N tends to infinity.

4.2 Neyman-Pearson detection with perfect observations

4.2.1 Observation model

Consider two probability measures $\mathbb{P}_0$ and $\mathbb{P}_1$ on a relevant probability space. Denote by $(Y_k)_{k\in\mathbb{Z}}$ a stationary ergodic process for both $\mathbb{P}_0$ and $\mathbb{P}_1$, taking its values in a bounded convex subset Y of $\mathbb{R}^d$. We associate an hypothesis ($\mathsf{H}0$ and $\mathsf{H}1$ respectively) to each of the two probability measures $\mathbb{P}_0$ and $\mathbb{P}_1$ and investigate the problem of the detection of $\mathsf{H}1$ vs. $\mathsf{H}0$ based on a set of n observations $Y_{1:n} = (Y_1, \ldots, Y_n)$.

For each $i \in \{0, 1\}$, we assume that $\mathbb{P}_i$ is the probability distribution of the coordinate process $(Y_k)_{k\in\mathbb{Z}}$ on the canonical space $(\mathsf{Y}^{\mathbb{Z}}, B(\mathsf{Y}^{\mathbb{Z}}))$. We denote by $P_{i,n}$ the restriction of $\mathbb{P}_i$ to $\sigma(Y_{1:n})$. We denote by $\mathbb{E}_0$ and $\mathbb{E}_1$ the expectations associated with $\mathbb{P}_0$ and $\mathbb{P}_1$ respectively. We introduce the reference measure μ which coincides with the d-dimensional Lebesgue measure restricted to Y.

Assumption 4.1 (Densities)**.** The following properties hold true for each $i \in \{0, 1\}$.

1. For each $n \geq 1$, $P_{i,n}$ admits a density p_i w.r.t. $\mu^{\otimes n}$.
2. $p_i(y_{1:n}) > 0$ for each $y_{1:n} \in \mathsf{Y}^n$.
3. $\mathbb{E}_0 \left|\log p_i(Y_0)\right| < \infty$.

The density p_i of $P_{i,n}$ depends of course on n, but we drop the index n to simplify the notation. For each $i \in \{0, 1\}$, we also define $p_i(y_n|y_{1:n-1}) = p_i(y_{1:n})/p_i(y_{1:n-1})$ with the convention that $p_i(y_n|y_{1:n-1}) = p_i(y_n)$ when $n = 1$ (that is, when $y_{1:n-1}$ is a void vector). Assumption 4.1.2 implies that both distributions $P_{0,n}$ and $P_{1,n}$ are absolutely continuous w.r.t. each other.

4.2.2 Likelihood ratio test

We now investigate the detection of $\mathsf{H}1$ vs. $\mathsf{H}0$ based on the perfect observation of n measurements $Y_{1:n}$. The log-likelihood ratio (LLR) writes:

$$L_n = \log \frac{p_1(Y_{1:n})}{p_0(Y_{1:n})} \,. \tag{4.1}$$

The NP test rejects the null hypothesis when L_n is larger than a threshold, say γ. For each $\alpha \in (0, 1)$, we define the miss probability of the NP test of level α by:

$$\beta_n(\alpha) = \inf \mathbb{P}_1 \left[L_n < \gamma\right] \,,$$

where the infimum is w.r.t. all γ such that the probability of false alarm does not exceed α i.e.,

$$\gamma \text{ s.t. } \mathbb{P}_0 \left[L_n > \gamma\right] \leq \alpha \,.$$

For each $n \geq 1$ and each $\alpha \in (0, 1)$, due to the celebrated Neyman-Pearson lemma, $\beta_n(\alpha)$ is the lowest achievable miss probability among all binary tests of level α which

are based on the observation of $Y_{1:n}$. Quantity $\beta_n(\alpha)$ is therefore a key metric in order to characterize the performance of the hypothesis test. Unfortunately, it usually does not admit any tractable closed-form expression. In the sequel, we study the asymptotic behavior of $\beta_n(\alpha)$ as the number of observations n tends to infinity. In this regime, it can be shown that, under certain assumptions,

$$\beta_n(\alpha) \simeq \exp(-n\,K) \tag{4.2}$$

for some constant K given below, which we shall refer to as the *error exponent*.

4.2.3 Error exponent with perfect observations

The evaluation of the error exponent K in (4.2) fundamentally relies on the following lemma, which can be found in [27].

Lemma 4.1 ([27]). *Assume that a binary test is performed on a sequence $\check{Y}_{1:n} = (\check{Y}_1, \dots, \check{Y}_n)$ of n observed random variables. Denote by $\check{p}_0$ and $\check{p}_1$ the density of $\check{Y}_{1:n}$ under* H0 *and* H1 *respectively (w.r.t. any common reference measure). Assume that under* H0*,*

$$\frac{1}{n} \log \frac{\check{p}_0(\check{Y}_{1:n})}{\check{p}_1(\check{Y}_{1:n})} \xrightarrow[n\to\infty]{P} \kappa$$

for some deterministic constant κ such that $0 < \kappa \leq \infty$. Then, for any $\alpha \in (0,1)$ the miss probability $\beta_n(\alpha)$ of the Neyman-Pearson test of level α is such that

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n(\alpha) = -\kappa\,.$$

Lemma 4.1 implies that the error exponent, if it exists, coincides with the limit in probability (under $\mathbb{P}_0$) of $-(1/n)L_n$, where L_n is the LLR defined by (4.1). The existence of the error exponent is directly obtained from the following assumption, which will be discussed later on.

Assumption 4.2 (Convergence)**.** For each $i \in \{0,1\}$, $(\log p_i(Y_0|Y_{-m:-1}))_{m\geq 0}$ is a convergent sequence in $L^1(\mathbb{P}_0)$.

We are now in position to study the limit of the LLR L_n and prove the following result, which provides the general form of the error exponent.

Theorem 4.2 (Error exponent)**.** *Under Assumptions 4.1 and 4.2,*

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n(\alpha) = -K\,,$$

where K is the constant defined by

$$K = \lim_{m\to\infty} \mathbb{E}_0 \left[\log \frac{p_0}{p_1}(Y_0|Y_{-m:-1}) \right]\,. \tag{4.3}$$

Proof. Using the chain rule, we first write L_n under the form:

$$L_n = -\sum_{k=1}^{n} \log \frac{p_0}{p_1}(Y_k|Y_{1:k-1}) \ .$$

Denote by Υ the limit in $L^1(\mathbb{P}_0)$ of sequence $(\log \frac{p_0}{p_1}(Y_0|Y_{-m:-1}))_{m\geq 0}$. The main point is the study of the difference $\log \frac{p_0}{p_1}(Y_k|Y_{1:k-1}) - \Upsilon \circ \theta^k$, where θ is the shift operator[1]. We can write:

$$\begin{aligned}\mathbb{E}_0 \left| \frac{1}{n} L_n + \frac{1}{n} \sum_{k=1}^{n} \Upsilon \circ \theta^k \right| &\overset{(a)}{\leq} \frac{1}{n} \sum_{k=1}^{n} \mathbb{E}_0 \left| \log \frac{p_0}{p_1}(Y_k|Y_{1:k-1}) - \Upsilon \circ \theta^k \right| \\ &\overset{(b)}{\leq} \frac{1}{n} \sum_{k=1}^{n} \mathbb{E}_0 \left| \log \frac{p_0}{p_1}(Y_0|Y_{-k+1:-1}) - \Upsilon \right| \ ,\end{aligned}$$

where step (a) comes from the triangular inequality and step (b) is a consequence of the stationarity of process $(Y_k)_{k\in\mathbb{Z}}$ under $\mathbb{P}_0$. The right-hand side of the above inequality can be interpreted as a Cesàro mean and thus converges to zero by definition of Υ:

$$-\frac{1}{n} L_n = \frac{1}{n} \sum_{k=1}^{n} \Upsilon \circ \theta^k + \varepsilon_n \ ,$$

where ε_n represents a term which converges in probability (under $\mathbb{P}_0$) to zero as n tends to ∞. As $\mathbb{P}_0$ is stationary ergodic, we conclude using the ergodic theorem that $-(1/n)L_n$ converges in probability to $\mathbb{E}_0(\Upsilon)$ under $\mathbb{P}_0$. This result together with Lemma 4.1 proves Theorem 4.2. □

Remark 4.1. Let us make some remarks on the above Assumptions 4.1 and 4.2. Assumption 4.1 is an extension of those made by Gupta and Hero [61, Section III, pp.1956]. Assumption 4.2 does not appear in [61] since it is obviously verified by i.i.d. processes. In this case, Theorem 4.2 is known as Stein's lemma. Assumption 4.2 is trivially satisfied by short-dependent (m-dependent) processes, such as moving average processes [20]. In this case, the present observation Y_0 is independent of past observations $Y_{-m-1}, Y_{-m-2}, \ldots$ as soon as m is large enough. As explained in Section 4.6, Assumption 4.2 is as well satisfied by a wide class of hidden Markov models.

Remark 4.2. In order that $(\log p_0(Y_0|Y_{-m:-1}))_{m\geq 0}$ is a convergent sequence in $L^1(\mathbb{P}_0)$, it is sufficient to check that $(\mathbb{E}_0 \log p_0(Y_0|Y_{-m:-1}))_{m\geq 0}$ is a bounded sequence. This claim is a consequence of Moy [110] (see Theorem 4 therein). In practical situations, this remark provides us with a convenient way to check whether Assumption 4.2 is verified for $i = 0$.

[1] Recall that we are considering probability measures defined on the canonical space $\mathsf{Y}^{\mathbb{Z}}$. For any $\omega \in \mathsf{Y}^{\mathbb{Z}}$, we may write $\omega = (\ldots, \omega_{-1}, \omega_0, \omega_1, \ldots)$. The kth-time shifted version of ω is then given by $\theta^k\omega = (\ldots, \omega_{k-1}, \omega_k, \omega_{k+1}, \ldots)$. Notation $\Upsilon \circ \theta^k$ represents the measurable function $\Upsilon \circ \theta^k(\omega) = \Upsilon(\theta^k\omega) = \Upsilon((\ldots, \omega_{k-1}, \omega_k, \omega_{k+1}, \ldots))$. Recall that process $Y_{\mathbb{Z}}$ is defined as the coordinate process i.e., $Y_n(\omega) = \omega_n$ for each n. As a consequence, the measurable function $\log \frac{p_0}{p_1}(Y_k|Y_{1:k-1}) - \Upsilon \circ \theta^k$ at point ω is equal to the measurable function $\log \frac{p_0}{p_1}(Y_0|Y_{-k+1:-1}) - \Upsilon$ at point $\theta^k\omega$.

On the other hand, the validation of Assumption 4.2 for $i = 1$ generally requires more efforts in practice: One should be able to prove that $(\log p_1(Y_0|Y_{-m:-1}))_{m\geq 0}$ is a Cauchy sequence in $L^1(\mathbb{P}_0)$.

Remark 4.3. When $\mathbb{P}_1$ is a finite-order Markovian measure, Assumption 4.2 can be simply reduced to the assumption that sequence $(\mathbb{E}_0 \log \frac{p_0}{p_1}(Y_0|Y_{-m:-1}))_{m\geq 0}$ is bounded. Indeed, due to Moy [110], this hypothesis directly implies the convergence of sequence $(\log \frac{p_0}{p_1}(Y_0|Y_{-m:-1}))_{m\geq 0}$ in $L^1(\mathbb{P}_0)$ and thus yields Theorem 4.2.

4.3 Quantization

4.3.1 Definitions

Consider a fixed integer $N \geq 2$. An N-point quantizer is a triplet $(\mathcal{C}_N, \Xi_N, \xi_N)$ where

- $\mathcal{C}_N = \{C_{N,1}, \ldots, C_{N,N}\}$ is a set of N *cells* (Borel sets of Y with non-zero volume) which form a partition of Y;
- $\Xi_N = \{\xi_{N,1}, \ldots, \xi_{N,N}\}$ is an arbitrary set of distinct elements; and
- $\xi_N : \mathsf{Y} \to \Xi_N$ is a function such that $\xi_N(y) = \xi_{N,j}$ whenever $y \in C_{N,j}$.

For each N, k, we introduce

$$Z_{N,k} = \xi_N(Y_k) \,,$$

the k-th quantized measurement on $\log_2(N)$ bits. We assume that the quantizer $(\mathcal{C}_N, \Xi_N, \xi_N)$ is known at the decision device. The aim is to decide between hypotheses $\mathsf{H}0$ and $\mathsf{H}1$ based on the observation of $Z_{N,1:n}$.

Note that in our model, each individual measurement is quantized based on the same quantization rule as in the traditional framework of vector-quantization [54]. It is also relevant in the case of WSN when samples are collected using identical sensors.

4.3.2 Error exponent with quantized observations

Assume that the number of quantization levels N is fixed. For a given number n of quantized observations, we define the LLR based on quantized measurements by:

$$L_{N,n} = \log \frac{p_{1,N}\left(Z_{N,1:n}\right)}{p_{0,N}\left(Z_{N,1:n}\right)} \,,$$

where for each $i \in \{0, 1\}$, and each quantization points $\xi_{N,j_{1:n}} = (\xi_{N,j_1}, \ldots, \xi_{N,j_n}) \in \Xi_N^n$,

$$p_{i,N}(\xi_{N,j_{1:n}}) = P_{i,n}(C_{N,j_1} \times \cdots \times C_{N,j_n})$$

is the probability that measurements $Y_1, \ldots, Y_n$ respectively fall into the cells $C_{N,j_1}, \ldots, C_{N,j_n}$ associated with the observed points $\xi_{N,j_1}, \ldots, \xi_{N,j_n}$ (n.b., function $p_{i,N}$ depends on n, but we omit the index n to simplify notation). We define similarly:

$$p_{i,N}(\xi_{N,j_n}|\xi_{N,j_{1:n-1}}) = \frac{p_{i,N}(\xi_{N,j_{1:n}})}{p_{i,N}(\xi_{N,j_{1:n-1}})} \,.$$

For each $\alpha \in (0,1)$, we denote by $\beta_{N,n}(\alpha)$ the miss probability of the NP test of level α when quantization is applied i.e., the infimum of $\mathbb{P}_1[L_{N,n} < \gamma]$ w.r.t. all γ s.t. $\mathbb{P}_0[L_{N,n} > \gamma] \leq \alpha$. The error exponent associated with $\beta_{N,n}(\alpha)$ is provided by the following result, whose proof is similar to the one of Theorem 4.2.

Corollary 4.3 (Error exponent with quantized observations)**.** *Consider a fixed $N \geq 2$. If Assumption 4.1 holds and if $(\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1}))_{m\geq 0}$ is a convergent sequence in $L^1(\mathbb{P}_0)$ for each $i \in \{0,1\}$ then,*

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_{N,n}(\alpha) = -K_N \ ,$$

where K_N is the constant defined by:

$$K_N = \lim_{m\to\infty} \mathbb{E}_0 \left[\log \frac{p_{0,N}}{p_{1,N}}(Z_{N,0}|Z_{N,-m:-1}) \right] \ . \tag{4.4}$$

The above result provides the error exponent K_N associated with the NP test on quantized observations. A natural question is: How does the choice of the quantizer affect the error exponent? Unfortunately, the expression of the error exponent does not immediately allow to evaluate the impact of the quantizer. In the sequel, we thus follow the approach of [61, 111] and focus on the case where the order N of the quantizer tends to infinity. We refer to such quantizers as *high-rate* quantizers. This approach leads to a convenient and informative asymptotic expression of K_N. In particular, it will be shown that, under some assumptions on the process $(Y_k)_{k\in\mathbb{Z}}$ and the quantizers sequence $(\mathcal{C}_N, \Xi_N, \xi_N)_{N\geq 1}$, the above error exponent K_N converges to K as N tends to infinity.

4.4 Performance of high-rate vector quantizers

4.4.1 Notation and assumptions

For each N, we remark that the error exponent K_N does not depend on the particular choice of the quantization alphabet Ξ_N.[2] For the sake of simplicity, we assume with no loss of generality that[3]:

$$\xi_{N,j} = \frac{\int_{C_{N,j}} y \, \mathrm{d}y}{\int_{C_{N,j}} \mathrm{d}y} \ ,$$

i.e., each $\xi_{N,j}$ coincides with the centroid of cell $C_{N,j}$. We respectively define the volume and the diameter of cell j by $V_{N,j} = \int_{C_{N,j}} \mathrm{d}y$ and $d_{N,j} = \sup_{u,v\in C_{N,j}} \|u - v\|$. We introduce

[2] The value of the log-likelihood ratio (and a fortiori the value of the error exponent) remains unchanged by any one-to-one transformation of the quantized observations. Otherwise stated, the particular definition of the quantization alphabet has no impact on the corresponding Neyman-Pearson test provided that the latter quantization alphabet is composed of N distinct elements.

[3] The ith component of $\xi_{N,j}$ is defined as $\xi_{N,j}^{(i)} \triangleq \left(\int_{C_{N,j}} y^{(i)} \, \mathrm{d}y\right) / \left(\int_{C_{N,j}} \mathrm{d}y\right)$.

the *specific point density* ζ_N and the *specific covariation profile* M_N as the piecewise constant functions on Y respectively defined as follows, for any $y \in C_{N,j}$ ($j \in \{1, \dots, N\}$):

$$\zeta_N(y) = \zeta_{N,j} = \frac{1}{NV_{N,j}} ,$$
$$M_N(y) = M_{N,j} = \frac{1}{V_{N,j}^{1+2/d}} \int_{C_{N,j}} (s - \xi_{N,j})(s - \xi_{N,j})^{\mathrm{T}} \, \mathrm{d}s .$$

Now consider a family of quantizers $(\mathcal{C}_N, \Xi_N, \xi_N)_{N \geq 1}$. We make the following assumption.

Assumption 4.3 (High-rate quantization)**.** The following properties hold true.

1. As N tends to ∞, ζ_N converges uniformly to a continuous function ζ such that $\inf_{y \in \mathsf{Y}} \zeta(y) > 0$.

2. As N tends to ∞, M_N converges uniformly to a continuous (matrix-valued) function M such that $\sup_{y \in \mathsf{Y}} \|M(y)\| < \infty$.

3. There exists a constant C_d such that, for all N, $\sup_j d_{N,j} \leq \dfrac{C_d}{N^{1/d}}$.

We will refer to ζ as the *model point density* of the family $(\mathcal{C}_N, \Xi_N, \xi_N)_{N \geq 1}$. It represents the fraction of cells in the neighborhood of a given point y. Function M will be referred to as the *model covariation profile*. For each $y \in \mathsf{Y}$, $M(y)$ is a non-negative $d \times d$ matrix. In the literature, function $y \mapsto \mathrm{Tr}\,(M(y))$ is usually referred to as the *inertial profile* [54, 61, 111]. Function M provides information about the shape of the cells.

Intuitively, high-rate quantizers should be constructed in such a way that $\zeta(y)$ is large at those points y for which a fine quantization is essential to discriminate the two hypotheses. Theorem 4.4 below provides a more rigorous formulation of this intuition.

Remark 4.4. Assumption 4.3 is essentially the same as the one traditionally made in the *high-rate quantization* framework [54,61,111]. The main difference lies in Assumption 4.3.3. Usually, the volume of each cell vanishes at speed $1/N$ while the diameter tends to zero. Our assumption introduces a constraint on the speed of convergence of the sequence of diameters $\{d_{N,j}\}$, which ensures that cells shrink at the same speed ($1/N^{1/d}$) on each dimension. Assumption 4.3 is for instance valid for sequence of quantizers constructed as *companders* [8, 54]. Such quantizers write as the composition of an invertible function (the so-called *compressor*) and a uniform quantizer. Since [8], it is known that any scalar quantizer can be written as a compander. Under mild conditions on the compressor, it can be shown that any sequence of companders with a given fixed compressor satisfies Assumption 4.3 (in this case, the model point density ζ is fully determined by the first order derivative of the compressor). This point is discussed in Section 4.4.3.

4.4.2 Error exponent in the high-rate regime

Before stating the main result, we need further assumptions. For each $m \geq 0$ and each $i \in \{0,1\}$, define:

$$\eta_i(m) = \sup_{m' \geq m} \mathbb{E}_0 \left| \log p_i(Y_0|Y_{-m:-1}) - \log p_i(Y_0|Y_{-m':-1}) \right| , \tag{4.5}$$

$$\eta_{i,N}(m) = \sup_{m' \geq m} \mathbb{E}_0 \left| \log p_{i,N}(Z_{N,0}|Z_{N,-m:-1}) - \log p_{i,N}(Z_{N,0}|Z_{N,-m':-1}) \right|$$

Note that we already assumed in Theorem 4.2 and Corollary 4.3 that sequences $\log p_i(Y_0|Y_{-m:-1})$ and $\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1})$ converge in $L^1(\mathbb{P}_0)$ as $m \to \infty$, meaning that $\eta_i(m)$ and $\eta_{i,N}(m)$ tend to zero. Now coefficients $\eta_i(m)$ and $\eta_{i,N}(m)$ characterize the speed at which $\log p_i(Y_0|Y_{-m:-1})$ and $\log p_{i,N}(Z_{N,0}|Z_{N,-m:-1})$ converge to their limits. They are therefore related to the mixing property of processes $Y_{\mathbb{Z}}$ and $Z_{N,\mathbb{Z}}$ (this point is discussed below in Remark 4.8). In the sequel, we will need to ensure that these limits are reached fast enough (see Assumption 4.4.3 below).

Assumption 4.4 (Smoothness and forgetting properties)**.** The following holds true:

1. For any $n \geq 1$, $y_{1:n} \mapsto p_i(y_{1:n})$ is of class C_3 on Y^n.
2. $\sup_{\{n \geq 1, y_{1:n} \in \mathsf{Y}^n,\, 1 \leq k,\ell,r \leq n,\, 1 \leq h,\bar{\imath},\bar{\jmath} \leq d\}} \left| \frac{\partial^3 \log p_i}{\partial y_k^{(h)} \partial y_\ell^{(\bar{\imath})} \partial y_r^{(\bar{\jmath})}}(y_{1:n}) \right| < \infty$.
3. There exist two constants C_e, $\epsilon > 0$ such that for each $i \in \{0,1\}$, $N \geq 2$ and $m \geq 0$,

$$\max \left\{ \eta_i(m) \, ; \eta_{i,N}(m) \right\} \leq \frac{C_e}{(1+m)^{6+\epsilon}} . \tag{4.6}$$

4. For each $i \in \{0,1\}$, each integers m, m', k such that $-m' \leq -m \leq 0 \leq k$:

$$\mathbb{E}_0 \left\| \nabla_{y_0} \log p_i(Y_{0:k}|Y_{-m:-1}) - \nabla_{y_0} \log p_i(Y_{0:k}|Y_{-m':-1}) \right\| \leq \varphi_m , \tag{4.7}$$

$$\mathbb{E}_0 \left\| \nabla_{y_0} \log p_i(Y_k|Y_{-m:k-1}) \right\| \leq \psi_k , \tag{4.8}$$

   where $\sum_k \varphi_k$ and $\sum_k \psi_k$ are convergent series.

Assumption 4.4 will be discussed in details at the end of the present subsection. Particular examples of processes satisfying the above assumption are provided in Section 4.6 and in the numerical results of Section 4.7.

We are now in position to state our main result. Recall that $p_0(y)$ is the p.d.f. of Y_0 under $\mathbb{P}_0$. Recall that K and K_N are the error exponents associated with the NP test in the absence and in the presence of quantization respectively, given by (4.3) and (4.4). Note that Assumption 4.4.3 implies that both sequences $\eta_i(m)$ and $\eta_{i,N}(m)$ tend to zero. This guarantees that under Assumption 4.1 the conclusions of Theorem 4.2 and Corollary 4.3 hold true i.e., error exponents K and K_N do exist.

Theorem 4.4. *Under Assumptions 4.1, 4.3, 4.4, the following statement holds true:*
As N tends to infinity, $N^{2/d}(K - K_N)$ converges to a constant D_e given by

$$D_e = \frac{1}{2} \int \frac{p_0(y)F(y)}{\zeta(y)^{2/d}} \, \mathrm{d}y \, , \tag{4.9}$$

where function F is given by

$$F(y) = \mathbb{E}_0 \left[\ell(Y_{\mathbb{Z}})^{\mathrm{T}} M(Y_0) \, \ell(Y_{\mathbb{Z}}) \, \middle| \, Y_0 = y \right] , \tag{4.10}$$

and random variable $\ell(Y_{\mathbb{Z}})$ is the limit in $L^2(\mathbb{P}_0)$ of sequence $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \right)_{k \geq 0}$.

Proof. See Section 4.5. □

Theorem 4.4 states that when the order of the quantizer tends to infinity, the error exponent K_N associated with the NP test converges at speed $N^{-2/d}$ to the error exponent K that one would have obtained in the absence of quantization. Loosely speaking, if $\beta_{N,n}(\alpha)$ represents the miss probability of the NP test of level α, the approximation

$$\beta_{N,n}(\alpha) \simeq e^{-n\left(K - \frac{D_e}{N^{2/d}}\right)} \tag{4.11}$$

holds when both the number n of sensors and the order N of quantization are large. Quantity D_e represents the (normalized) loss in error exponent between the quantized and the unquantized cases, in the high-rate quantization regime.

Note that (4.9) resembles Bennett's formula [8, Eq. (1.6)] and its vector extension for rth-power distortion [111, Eq. (7)].

Remark 4.5. As a first consequence of Theorem 4.4, under some assumptions on the process, *classical* quantizers as those produced in an MSE perspective will lead to error exponent K_N which converges to K as N tends to infinity, at speed $N^{-2/d}$ (see (4.11) above).

Remark 4.6. The particular situation where measurements $(Y_k)_{k \geq 0}$ are i.i.d. under both hypotheses was studied by Gupta and Hero [61]. In this case, function $F(y)$ reduces to:

$$F(y) = \nabla \Lambda(y)^{\mathrm{T}} \, M(y) \, \nabla \Lambda(y) \, ,$$

where $\Lambda(y) = \log \frac{p_0(y)}{p_1(y)}$ is the single sample LLR. Expression (4.9) of D_e is then consistent with the results of Gupta and Hero (see in particular [61, Eq. (20)]). Note also that we assume that each joint density $p_0(y_{1:n})$ and $p_1(y_{1:n})$ is of class C_3 on Y^n. Gupta and Hero's assumption is weaker, since they only assume that "*the densities are twice continuously differentiable on an open set of probability* 1" [61, page 1956]. In fact, we need conditions on the third derivatives of the logarithm of the densities in order to find relevant upper bounds of the Taylor-Lagrange remainders in the expansion of the *joint* densities $p_i(y_{-m:u})$ in the general case (see the detailed proof in Section 4.5).

Remark 4.7. We now provide some insights on the meaning of Assumption 4.4 and on the class of stationary processes which satisfy the latter. Assumptions 4.4.1 and 4.4.2 are mild technical conditions on the smoothness of the p.d.f. of the observations. They encompass a large family of stochastic processes and are generally simple to validate on a case-by-case basis. As explained above, Assumption 4.4.3 can be interpreted as a condition on the speed at which past observations are forgotten. Quantities $\eta_i(m)$ and $\eta_{i,N}(m)$ can be interpreted as conditional mixing coefficients associated with the unquantized and quantized processes $(Y_k)_k$ and $(Z_{N,k})_k$ respectively (see Remark 4.8 below). Past observations must be forgotten at least at a polynomial speed faster than m^6. Assumption 4.4.4 can be interpreted similarly as a forgetting property, which no longer involves the logarithm of the density of the observations, but its derivative. For instance, Assumption 4.4 is simple to verify in case of short-dependent processes (such as moving average processes) provided that the density of the observations is smooth enough. A similar remark holds for a wide class of Markov chains. In this case, Assumption 4.4 essentially reduces to a smoothness assumption on the density of the transition kernel. More generally, we prove in Section 4.6 that Assumption 4.4 holds for a wide class of hidden Markov models: We provide sufficient conditions on the transition kernel such that Assumption 4.4 holds. See also the numerical results in Section 4.7.

Remark 4.8. It is worth making some remarks on the link between Assumption 4.4 and standard mixing conditions used in the literature on mixing processes [19, 20, 38]. The mixing property which is the closest to our setting is related to the notion of ψ-mixing. For two σ-fields $\mathcal{U}$ and $\mathcal{V}$, define the following coefficient [20, 38]:

$$\psi(\mathcal{U},\mathcal{V}) = \sup_{\substack{U\in\mathcal{U},V\in\mathcal{V}\\ \mathbb{P}(U)>0,\mathbb{P}(V)>0}} \left|1 - \frac{\mathbb{P}(U\cap V)}{\mathbb{P}(U)\,\mathbb{P}(V)}\right| .$$

Recall that a stochastic process $Y_{\mathbb{Z}}$ is said to be ψ-mixing when the sequence of ψ-mixing coefficients $\psi(\sigma(Y_{n+1}), \sigma(Y_{-\infty:0}))$ converges to zero. The classical ψ-mixing condition traduces the fact that, loosely speaking, current samples at time n tend to become independent of past samples $Y_0, Y_{-1}, \ldots$ as n increases. In our case, we need to ensure that current samples become independent of past ones *conditionally to intermediate values* $Y_{1:n}$. Usual ψ-mixing coefficient do not fully allow to grasp this property. We can introduce the following *conditional* ψ-mixing coefficient for σ-fields $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{W}$:

$$\bar{\psi}_i(\mathcal{U},\mathcal{V}|\mathcal{W}) = \sup_{U\in\mathcal{U},\,V\in\mathcal{V}} \operatorname{ess\,sup} \left|1 - \frac{\mathbb{P}_i(U\cap V|\mathcal{W})}{\mathbb{P}_i(U|\mathcal{W})\,\mathbb{P}_i(V|\mathcal{W})}\right|$$

where the essential supremum is taken w.r.t. $\mathbb{P}_0$ and where we use the convention $0/0 = 1$. The above coefficient can be interpreted as a measure of dependence (under $\mathbb{P}_i$) between $\mathcal{U}$ and $\mathcal{V}$ conditionally to $\mathcal{W}$. In particular, it coincides with the traditional ψ-mixing coefficient $\psi(\mathcal{U},\mathcal{V})$ when $\mathcal{W}$ is taken to be the whole space $B(\mathsf{Y}^{\mathbb{Z}})$ and $\mathbb{P} = \mathbb{P}_0$. For each $n \geq 1$, we further define $\bar{\psi}_i(n) = \bar{\psi}_i(\sigma(Y_{n+1}), \sigma(Y_{-\infty:0})|\sigma(Y_{1:n}))$ and $\bar{\psi}_i(0) = \bar{\psi}_i(\sigma(Y_1), \sigma(Y_{-\infty:0}))$

when $n = 0$. There exists a close link between the above conditional mixing coefficients and the set of coefficients $\eta_i(m)$ defined in (4.5). In particular, Theorem 2 is valid when Assumption 4.4.2 is replaced by the assumption that sequences $\bar{\psi}_1(n)$ and $\bar{\psi}_{i,N}(n) = \bar{\psi}_i(\sigma(Z_{N,n+1}), \sigma(Z_{N,-\infty:0})|\sigma(Z_{N,1:n}))$ converge to zero at speed $n^{6+\epsilon}$.

The asymptotic loss in error exponent D_e depends on the quantizer through its model point density ζ and its model covariation profile M. In the sequel, we study the values of these parameters which attenuate as much as possible the loss D_e.

4.4.3 Determination of relevant high-rate quantizers: Scalar case ($d = 1$)

We first address the case where measurements $(Y_k)_{k\geq 0}$ are real-valued. Assume without much loss of generality that each cell is connected (cells are intervals) i.e., the quantizer is regular [50]. In this case, a straightforward derivation leads to $M_N(y) = 1/12$ for each y and each N. Therefore, function F simplifies to:

$$\begin{aligned} F(y) &= \frac{1}{12}\,\mathbb{E}_0\left[\ell(Y_{\mathbb{Z}})^2 \,\middle|\, Y_0 = y\right] \\ &= \frac{1}{12}\lim_{k\to\infty}\mathbb{E}_0\left[\left(\frac{\partial}{\partial y_0}\log\frac{p_0}{p_1}(Y_{-k:k})\right)^2 \,\middle|\, Y_0 = y\right]. \end{aligned}$$

Using Hölder's inequality on (4.9), it is straightforward to prove the following result.

Corollary 4.5. *Assume that $d = 1$ and that cells are intervals. The error exponent loss D_e is such that:*

$$D_e \geq \frac{1}{2}\left(\int [p_0(y)F(y)]^{1/3}\,\mathrm{d}y\right)^3. \tag{4.12}$$

Equality holds in (4.12) *when the model point density coincides with:*

$$\zeta(y) = \frac{[p_0(y)F(y)]^{1/3}}{\int [p_0(s)F(s)]^{1/3}\,\mathrm{d}s}.$$

The above corollary provides the optimal high-rate quantization rule for the initial hypothesis testing problem. Note that expression (4.12) is quite similar to [122, Eq. (15)] which gives "the minimum distortion resulting with optimum level spacing" in an MSE perspective.

Remark 4.9. In practice, N-point scalar quantizer achieving a given model point density ζ can be easily implemented by means of a compander. Recall that a compander is defined as the composition of an invertible continuous function ϕ (the so-called compressor) and a uniform quantizer [8, 54]. To that end, it is sufficient to define the compressor ϕ as the primitive of ζ on the observation space. For example, if Y is the segment $[a, b] \subset \mathbb{R}$, define $\phi(x) = \int_a^x \zeta(t)\,\mathrm{d}t$. Next, the output of the compressor is quantized using a uniform N-point quantizer on the interval $[0, 1]$. Under the assumption that ζ is a Lipschitz function, it is straightforward to show that the resulting sequence of quantizers satisfies Assumption 4.3 i.e., that it achieves the model point density ζ.

4.4.4 Determination of relevant high-rate quantizers: Vector case ($d \geq 2$)

In the vector case, the determination of optimal high-rate quantization rules implies the joint minimization of expression (4.9) w.r.t. both functions ζ and M. Unfortunately, as remarked in [54, 116], it is not known what functions M are allowable as covariation profiles. The determination of the set of admissible couples (ζ, M) is an open problem, which is beyond the scope of this thesis.

However, when M is fixed, the point density ζ which minimizes D_e can be easily expressed as a function of M. Once again, this is a consequence of Hölder's inequality:

$$D_e \geq \frac{1}{2} \left(\int [p_0(y) F(y)]^{\frac{d}{d+2}} \, \mathrm{d}y \right)^{\frac{d+2}{d}} ,$$

where equality is achieved when the point density coincides with:

$$\zeta(y) = \frac{[p_0(y) F(y)]^{\frac{d}{d+2}}}{\int [p_0(s) F(s)]^{\frac{d}{d+2}} \, \mathrm{d}s} . \tag{4.13}$$

In other words, one can easily provide the optimal high-rate quantization rule for a given limiting covariation profile. Following the approach of [61], we study two special cases of covariation profile.

4.4.4.1 Congruent cells with minimum moment of inertia

In this paragraph, we focus on congruent cells with minimum moment of inertia i.e., we assume that

$$\forall\, y \in \mathsf{Y},\ M(y) = \nu I_d \, , \tag{4.14}$$

for some $\nu > 0$, where I_d represents the $d \times d$ identity matrix.

Recall that Gersho [49] made the now widely accepted conjecture that when N tends to infinity, most cells (i.e., all the cells except those which are close to the boundary of the considered domain) of a d-dimensional MSE-optimal quantizer become congruent to some tessellating d-dimensional polytope H_d^*. In such a case, $M(y)$ is independent of y. Furthermore, Zamir and Feder [173, Lemma 1] proved that the cells of the MSE-optimal lattice quantizers become "closer" to balls i.e., with minimum moment of inertia, as dimension d grows.

For quantizers with covariation profile given by (4.14), the optimal point density (4.13) becomes:

$$\zeta(y) = \frac{\left[p_0(y) \bar{F}(y)\right]^{\frac{d}{d+2}}}{\int \left[p_0(s) \bar{F}(s)\right]^{\frac{d}{d+2}} \, \mathrm{d}s} , \tag{4.15}$$

where function $\bar{F}$ is defined by

$$\begin{aligned} \bar{F}(y) &= \mathbb{E}_0 \left[\|\ell(Y_{\mathbb{Z}})\|^2 \,\middle|\, Y_0 = y \right] \\ &= \lim_{k \to \infty} \mathbb{E}_0 \left[\left\| \nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \right\|^2 \,\middle|\, Y_0 = y \right] . \end{aligned} \tag{4.16}$$

Design Algorithm. In practice, one would like to design an N-point quantizer which point density approximately equals (4.15) for some finite N. This can be achieved by means of well-established algorithms, the most popular of them being the Linde-Buzo-Gray (LBG) algorithm [93]. This algorithm is an iterative method which computes a Voronoi tessellation, and yields an MSE-optimal N-point quantizer, from a training set of data of some p.d.f. $p_0(y)$.

An (N-point) MSE-optimal quantizer for density p_0 minimizes $\mathbb{E}_0\left[\|Y_0 - \xi_N(Y_0)\|^2\right]$. As the number of quantization points N tends to infinity, such a quantizer has the following model point density [54, 111]:

$$\zeta_{MSE}(y) = \frac{p_0(y)^{\frac{d}{d+2}}}{\int p_0(s)^{\frac{d}{d+2}}\,\mathrm{d}s}\,. \tag{4.17}$$

Comparing (4.15) and (4.17), we deduce that the proposed quantizer, whose model point density ζ is given by (4.15), can be obtained in practice by simply feeding the classical LBG algorithm with a training set of data of the following p.d.f.:

$$q^*(y) = \frac{p_0(y)\bar{F}(y)}{\int p_0(s)\bar{F}(s)\,\mathrm{d}s}\,.$$

Section 4.7 provides numerical illustrations of this approach.

4.4.4.2 Ellipsoidal cells

In order to yield some insights on the general shape of the cells, and following [61], we focus in this paragraph on ellipsoidal cells. This kind of cells cannot partition the considered convex subset Y of $\mathbb{R}^d$ but, for large dimension d, in analogy with the spherical cell approximation [29, 54, 173], we may assume that almost all cells of a given quantizer are close to ellipsoids.

Such an ellipsoidal cell, in the neighborhood of point y writes $C = \{x : (x-y)^{\mathrm{T}} R(y)\,(x-y) \leq 1\}$, for some symmetric positive definite matrix $R(y)$. The corresponding covariation profile writes $M(y) = \nu\,|R(y)|^{1/d}\,R(y)^{-1}$ [60, 61], for some $\nu > 0$, and has an eigendecomposition

$$M(y) = U(y)\,\Phi(y)\,U(y)^{\mathrm{T}}\,,$$

where $\Phi(y) = \mathrm{Diag}\,(\phi_{1:d}(y))$,[4] and $U(y)$ is an orthogonal matrix. Note that the (positive) eigenvalues $(\phi_i(y))_{i\in\{1,\ldots,d\}}$ of $M(y)$ capture the relative importance of the axes of the ellipsoid C, while the columns $(u_i(y))_{i\in\{1,\ldots,d\}}$ of $U(y)$ i.e., the eigenvectors of $M(y)$, indicate their respective directions.

In this paragraph, we assume that eigenvalues $(\phi_i)_{i\in\{1,\ldots,d\}}$ are fixed, constant w.r.t. y and, without loss of generality, sorted in increasing order i.e., $0 < \phi_1 \leq \phi_2 \leq \cdots \leq \phi_d$. We want to find the best orthogonal matrix $U(y)$ i.e., the one which minimizes function $F(y)$,

[4] For any given d-dimensional vector $x_{1:d} \in \mathbb{R}^d$, $\mathrm{Diag}\,(x_{1:d})$ represents the d-by-d diagonal matrix with diagonal coefficients $(x_1, x_2, \ldots, x_d)$.

given at (4.10), in order to minimize the error exponent loss D_e (4.9). In other words, for a given "shape" of (non-degenerate) ellipsoid, we look for the best directions of its axes. Function $F(y)$ writes:

$$\begin{aligned} F(y) &= \mathbb{E}_0 \left[\ell(Y_{\mathbb{Z}})^{\mathrm{T}} M(Y_0)\, \ell(Y_{\mathbb{Z}}) \,\middle|\, Y_0 = y \right] \\ &= \mathrm{Tr}\left(U(y)\, \Phi\, U(y)^{\mathrm{T}} \bar{L}(y) \right) , \end{aligned} \tag{4.18}$$

where $\bar{L}(y) = \mathbb{E}_0 \left[\ell(Y_{\mathbb{Z}})\, \ell(Y_{\mathbb{Z}})^{\mathrm{T}} \,\middle|\, Y_0 = y \right]$. Now write the eigendecomposition of the positive definite matrix $\bar{L}(y)$:

$$\bar{L}(y) = V(y)\, \Delta(y)\, V(y)^{\mathrm{T}} ,$$

where $\Delta(y) = \mathrm{Diag}\,(\lambda_{1:d}(y))$; $(\lambda_i(y))_{i\in\{1,\dots,d\}}$ are the (positive) eigenvalues of $\bar{L}(y)$ sorted in increasing order i.e., $0 < \lambda_1(y) \leq \lambda_2(y) \leq \cdots \leq \lambda_d(y)$; and $V(y)$ is an orthogonal matrix. Equation (4.18) thus writes:

$$\begin{aligned} F(y) &= \mathrm{Tr}\left(U(y)\, \Phi\, U(y)^{\mathrm{T}} V(y)\, \Delta(y)\, V(y)^{\mathrm{T}} \right) \\ &\geq \sum_{i=1}^{d} \phi_i\, \lambda_{d-i+1}(y) , \end{aligned}$$

where the last inequality follows from a well-known trace inequality for positive semidefinite Hermitian matrices [85], [102, Section 9-H]. The above lower bound is furthermore achieved choosing matrix $U(y)$ such that $U(y)^{\mathrm{T}} V(y)$ is the anti-diagonal matrix with ones on its anti-diagonal i.e., defining the ith column of matrix $U(y)$ as the $(d-i+1)$th column of matrix $V(y)$, or equivalently eigenvector $u_i(y)$ of matrix $M(y)$ as eigenvector $v_{d-i+1}(y)$ of matrix $\bar{L}(y)$.

From the above derivations, we conclude that if a cell is a non-degenerate ellipsoid around y then its axes should be aligned along the ones of matrix $\bar{L}(y)$ in the reverse order. In particular, its minor axis should be aligned along the principal eigenvector of matrix $\bar{L}(y)$.

4.5 Proof of Theorem 4.4

4.5.1 Preliminaries

Recall that $V_{N,j} = \int_{C_{N,j}} \mathrm{d}y$ is the volume of cell $C_{N,j}$ ($j \in \{1,\dots,N\}$). For each $i \in \{0,1\}$ and each set of quantization points $\xi_{N,j_{1:n}} = (\xi_{N,j_1},\dots,\xi_{N,j_n}) \in \Xi_N^n$, define the following rescaled p.d.f. of $Z_{N,1:n}$:

$$\begin{aligned} \bar{p}_{i,N}(\xi_{N,j_{1:n}}) &= \frac{1}{V_{N,j_1} \times \cdots \times V_{N,j_n}}\, p_{i,N}(\xi_{N,j_{1:n}}) \\ &= \frac{1}{V_{N,j_1} \times \cdots \times V_{N,j_n}}\, P_{i,n}(C_{N,j_1} \times \cdots \times C_{N,j_n}) . \end{aligned} \tag{4.19}$$

The above definition is convenient because $\bar{p}_{i,N}(\xi_{N,j_{1:n}}) \simeq p_i(\xi_{N,j_{1:n}})$ for large values of N. This approximation will be of prime importance in the sequel. We define function $\bar{p}_{i,N}(\xi_{N,j_n}|\xi_{N,j_{1:n-1}})$ similarly.

For each $i \in \{0,1\}$ and each integer $\ell \geq 0$, we introduce the following functions:

$$\begin{aligned} &\forall\, y_{-\ell:0} \in \mathsf{Y}^{\ell+1}, \qquad \mathcal{L}_i(y_{-\ell:0}) = \log p_i(y_0|y_{-\ell:-1}) \,, \\ &\forall\, z_{-\ell:0} \in \Xi_N^{\ell+1}, \quad \mathcal{L}_{i,N}(z_{-\ell:0}) = \log \bar{p}_{i,N}(z_0|z_{-\ell:-1}) \,. \end{aligned}$$

Due to Assumptions 4.1.3 and 4.4.3 (which ensures that $\eta_i(0) < \infty$), random sequence $(\mathcal{L}_i(Y_{-\ell:0}))_{\ell\geq 0}$ lies in $L^1(\mathbb{P}_0)$. Moreover, Assumption 4.4.3 for large m ensures that sequence $(\mathcal{L}_i(Y_{-\ell:0}))_{\ell\geq 0}$ is a Cauchy sequence of $L^1(\mathbb{P}_0)$. Denote by $\mathcal{L}_i(Y_{-\infty:0})$ its limit. From Assumption 4.4.3 once again, the following holds for any $\ell \geq 0$,

$$\mathbb{E}_0|\mathcal{L}_i(Y_{-\ell:0}) - \mathcal{L}_i(Y_{-\infty:0})| \leq \frac{C_e}{(1+\ell)^{\,6+\epsilon}} \,. \tag{4.20}$$

A similar result holds for sequence $(\mathcal{L}_{i,N}(Z_{N,-\ell:0}))_{\ell\geq 0}$ which converges in $L^1(\mathbb{P}_0)$ to some random variable $\mathcal{L}_{i,N}(Z_{N,-\infty:0})$ and verifies for any $\ell \geq 0$,

$$\mathbb{E}_0|\mathcal{L}_{i,N}(Z_{N,-\ell:0}) - \mathcal{L}_{i,N}(Z_{N,-\infty:0})| \leq \frac{C_e}{(1+\ell)^{\,6+\epsilon}} \,. \tag{4.21}$$

Our aim is to study the difference $K - K_N$ between error exponents associated with the ideal and quantized cases respectively. We may write the difference as

$$K - K_N = (K_0 - K_{0,N}) - (K_1 - K_{1,N}) \,, \tag{4.22}$$

where we defined for each $i \in \{0,1\}$,

$$\begin{aligned} K_i &= \mathbb{E}_0\left[\mathcal{L}_i(Y_{-\infty:0})\right] \,, \\ K_{i,N} &= \mathbb{E}_0\left[\mathcal{L}_{i,N}(Z_{N,-\infty:0})\right] \,. \end{aligned}$$

In the sequel, we focus on the study of $K_1 - K_{1,N}$, the study of $K_0 - K_{0,N}$ being similar.

We now proceed with the proof. Choose any ϵ' such that $0 < \epsilon' < \frac{\epsilon}{3d(6+\epsilon)}$. Define the sequence of integers $m = m(N) = \lfloor N^{1/(3d)-\epsilon'} \rfloor$. We shall remember that with this definition,

$$\lim_{N\to\infty} \frac{m^3}{N^{1/d}} = 0 \,. \tag{4.23}$$

The following decomposition holds true: $K_{1,N} = K_1 + T_N + U_N + \delta_N$, where we defined:

$$\begin{aligned} T_N &= \mathbb{E}_0\left[\mathcal{L}_{1,N}(Z_{N,-m:0}) - \mathcal{L}_1(Z_{N,-m:0})\right] \,, \\ U_N &= \mathbb{E}_0\left[\mathcal{L}_1(Z_{N,-m:0}) - \mathcal{L}_1(Y_{-m:0})\right] \,, \\ \delta_N &= \mathbb{E}_0\left[\mathcal{L}_{1,N}(Z_{N,-\infty:0}) - \mathcal{L}_{1,N}(Z_{N,-m:0})\right] + \mathbb{E}_0\left[\mathcal{L}_1(Y_{-m:0}) - \mathcal{L}_1(Y_{-\infty:0})\right] \,. \end{aligned}$$

Using (4.20) and (4.21), it is straightforward to show that

$$N^{2/d}|\delta_N| \leq 2\, C_e\, \frac{N^{2/d}}{(1+m)^{\,6+\epsilon}}\,.$$

By definition of $m = m(N)$, we deduce that $N^{2/d}|\delta_N|$ converges to zero as $N \to \infty$. As a consequence, the asymptotic analysis of quantity $N^{2/d}(K_{1,N} - K_1)$ reduces to the study of T_N and U_N.

As Y is a bounded set, Assumption 4.4.2 implies the following bounds on the derivatives of density p_1 which will be of permanent use in the sequel:

$$\sup_{\{y_{1:n}\in\mathsf{Y}^n,\, 1\leq k\leq n\}} \|\nabla_{y_k} \log p_1(y_{1:n})\| \leq C_1\,, \tag{4.24}$$

$$\sup_{\{y_{1:n}\in\mathsf{Y}^n,\, 1\leq k\leq n\}} \left\|\nabla^2_{y_k} \log p_1(y_{1:n})\right\| \leq C_2\,, \tag{4.25}$$

for some constants C_1 and C_2.

4.5.2 Study of T_N

We expand T_N as follows:

$$T_N = \mathbb{E}_0\left[\log \frac{\bar{p}_{1,N}(Z_{N,-m:0})}{p_1(Z_{N,-m:0})}\right] - \mathbb{E}_0\left[\log \frac{\bar{p}_{1,N}(Z_{N,-m:-1})}{p_1(Z_{N,-m:-1})}\right]\,. \tag{4.26}$$

We now study each term of the r.h.s. of the above equality. Consider $u \in \{-1, 0\}$. Writing the Taylor-Lagrange expansion of function $y_{-m:u} \mapsto p_1(y_{-m:u})$ at point $\xi_{N,j_{-m:u}}$, using Assumptions 4.3.3, 4.4 and the properties of the quantizers sequence, we can prove the following lemma.

Lemma 4.6. *For each $j_{-m:u} \in \{1,\dots,N\}^{u+m+1}$, the following expansion holds true:*

$$\frac{\bar{p}_{1,N}(\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} = 1 + \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathit{Tr}\left(\frac{\nabla^2_{y_k} p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}}}{p_1(\xi_{N,j_{-m:u}})}\, \frac{M_{N,j_k}}{\zeta_{N,j_k}^{2/d}}\right) + \epsilon_{N,j_{-m:u}}\,,$$

where $\left|\epsilon_{N,j_{-m:u}}\right| \leq c_T \left(\frac{m+1}{N^{1/d}}\right)^3$ for some constant c_T.

Proof. See Appendix F.1. □

Plugging the above equation into (4.26), using $\left|\log(1+x) - x\right| \leq x^2$ in a neighborhood of zero, Assumptions 4.3, 4.4.2, and (4.23), we obtain:

$$T_N = T_N(0) - T_N(-1) + o_N(N^{-2/d})\,, \tag{4.27}$$

where, for each $u \in \{-1, 0\}$,

$$T_N(u) = \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0\left[\mathrm{Tr}\left(\frac{\nabla^2_{y_k} p_1(Z_{N,-m:u})^{\mathrm{T}}}{p_1(Z_{N,-m:u})}\, \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}}\right)\right]\,. \tag{4.28}$$

4.5.3 Study of U_N

We expand U_N as follows:

$$U_N = \mathbb{E}_0\big[\log p_1(Z_{N,-m:0}) - \log p_1(Y_{-m:0})\big] - \mathbb{E}_0\big[\log p_1(Z_{N,-m:-1}) - \log p_1(Y_{-m:-1})\big] , \tag{4.29}$$

and study each term of the r.h.s. of the above equality. For each $u \in \{-1, 0\}$ and each $j_{-m:u} \in \{1, \dots, N\}^{u+m+1}$, we expand function $y_{-m:u} \mapsto \log p_1(y_{-m:u})$ at point $\xi_{N,j_{-m:u}}$:

$$\begin{aligned}\log p_1(y_{-m:u}) = \log p_1(\xi_{N,j_{-m:u}}) + \sum_{k=-m}^{u} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} (y_k - \xi_{N,j_k}) \\ + \frac{1}{2} \sum_{k,\ell=-m}^{u} (y_k - \xi_{N,j_k})^{\mathrm{T}} \nabla^2_{y_k,y_\ell} \log p_1(\xi_{N,j_{-m:u}}) (y_\ell - \xi_{N,j_\ell}) + \epsilon'_N(y_{-m:u}) . \end{aligned} \tag{4.30}$$

Under Assumptions 4.33 and 4.4.2, for each $y_{-m:u} \in C_{N,j_{-m}} \times \cdots \times C_{N,j_u}$, the remainder is such that

$$\big|\epsilon'_N(y_{-m:u})\big| \le (m+1)^3 \, c'_3 \left(\frac{C_d}{N^{1/d}}\right)^3 ,$$

for some constant c'_3. By (4.23), the r.h.s. of the above inequality converges to zero as N tends to infinity faster than $N^{-2/d}$. Plugging Taylor expansion (4.30) into the expression (4.29) of U_N, we obtain:

$$U_N = U_N(0) - U_N(-1) + o_N(N^{-2/d}) , \tag{4.31}$$

where, for each $u \in \{-1, 0\}$,

$$\begin{aligned} U_N(u) = - \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} (Y_k - Z_{N,k})\right] \\ - \frac{1}{2} \sum_{k,\ell=-m}^{u} \mathbb{E}_0 \left[(Y_k - Z_{N,k})^{\mathrm{T}} \nabla^2_{y_k,y_\ell} \log p_1(Z_{N,-m:u}) (Y_\ell - Z_{N,\ell})\right] . \end{aligned} \tag{4.32}$$

The next step is to study each dominant term of the r.h.s. of (4.32).

Lemma 4.7. *The following equality holds true for each $u \in \{-1, 0\}$:*

$$U_N(u) = A_N(u) + B_N(u) + o_N(N^{-2/d}) ,$$

where A_N and B_N are defined as follows:

$$A_N(u) = -\frac{1}{N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:u})\right] , \tag{4.33}$$

$$B_N(u) = -\frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[Tr\left(\nabla^2_{y_k} \log p_1(Z_{N,-m:u}) \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}}\right)\right] .$$

Proof. See Appendix F.2. □

Now we expand the term $\nabla^2_{y_k} \log p_1$ as follows:

$$\nabla^2_{y_k} \log p_1(y_{-m:u}) = \frac{\nabla^2_{y_k} p_1(y_{-m:u})}{p_1(y_{-m:u})} - \frac{\nabla_{y_k} p_1(y_{-m:u}) \nabla_{y_k} p_1(y_{-m:u})^{\mathrm{T}}}{(p_1(y_{-m:u}))^2} .$$

From the above decomposition and (4.28), we can divide $B_N(u)$ into two terms:

$$B_N(u) = -T_N(u) + \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\mathrm{Tr} \left(\nabla_{y_k} \log p_1(Z_{N,-m:u}) \nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \right) \right] . \quad (4.34)$$

Expanding function $\nabla_{y_k} \log p_1$ in the above equation and in (4.33), we can write dominant terms in a simple form i.e., replace each Z_N by Y. Under Assumption 4.3, from (4.25) and (4.23), we can easily prove that the corresponding remainders are $o_N(N^{-2/d})$.

Putting all pieces together, we obtain

$$\begin{aligned} U_N(u) = &- \frac{1}{N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:u}) \right] \\ &+ \frac{1}{2N^{2/d}} \sum_{k=-m}^{u} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_1(Y_{-m:u}) \right] \\ &- T_N(u) + o_N(N^{-2/d}) . \end{aligned} \quad (4.35)$$

4.5.4 End of proof

From the results of Sections 4.5.2 and 4.5.3, we can easily prove the following lemma.

Lemma 4.8. *The following holds true:*

$$N^{2/d}(K - K_N) = \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-m:0}) \right] + \sum_{k=-m}^{-1} \mathbb{E}_0 \left[\mathcal{H}_{N,k}(Y_{-m:0}) - \mathcal{H}_{N,k}(Y_{-m:-1}) \right] + o_N(1) , \quad (4.36)$$

where for each $u \in \{-1, 0\}$, each $m \geq 1$ and each $k \in \{-m, \ldots, u\}$:

$$\mathcal{H}_{N,k}(Y_{-m:u}) = \frac{1}{2} \nabla_{y_k} \log \frac{p_0}{p_1}(Y_{-m:u})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log \frac{p_0}{p_1}(Y_{-m:u}) . \quad (4.37)$$

Proof. Recalling the decomposition $K_{1,N} = K_1 + T_N + U_N + o_N(N^{-2/d})$ and gathering

(4.27), (4.31), (4.35), it is straightforward to prove the following equality:

$$\begin{aligned} N^{2/d}(K_{1,N} - K_1) = & - \sum_{k=-m}^{0} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:0})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:0}) \right] \\ & + \frac{1}{2} \sum_{k=-m}^{0} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:0})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_1(Y_{-m:0}) \right] \\ & + \sum_{k=-m}^{-1} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:-1})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_0(Y_{-m:-1}) \right] \\ & - \frac{1}{2} \sum_{k=-m}^{-1} \mathbb{E}_0 \left[\nabla_{y_k} \log p_1(Y_{-m:-1})^{\mathrm{T}} \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \nabla_{y_k} \log p_1(Y_{-m:-1}) \right] \\ & + o_N(1) \, . \end{aligned}$$

Similar expression holds for $N^{2/d}(K_{0,N} - K_0)$–replace all p_1 by p_0 in the above equation. Lemma 4.8 follows from decomposition (4.22). □

We now study the series (4.36). From Assumptions 4.3, 4.4.2 and 4.4.4, the following forgetting properties hold true for any positive integers ℓ', ℓ and any integers k, u such that $-\ell' \leq -\ell \leq k \leq u$:

$$\mathbb{E}_0 \left| \mathcal{H}_{N,k}(Y_{-\ell:u}) - \mathcal{H}_{N,k}(Y_{-\ell':u}) \right| \leq c_h \varphi_{\ell - |k|} \, , \tag{4.38}$$

$$\mathbb{E}_0 \left| \mathcal{H}_{N,k}(Y_{-\ell:0}) - \mathcal{H}_{N,k}(Y_{-\ell:-1}) \right| \leq c_h \psi_{|k|} \, , \tag{4.39}$$

for some constant c_h.

It is clear from (4.38) that sequence $(\mathcal{H}_{N,k}(Y_{-\ell:u})))_{\ell \geq -u}$ is a Cauchy sequence in $L^1(\mathbb{P}_0)$. We simply denote its limit by $\mathcal{H}_{N,k}(Y_{-\infty:u})$. Inequalities (4.38) and (4.39) provide the main tools for the asymptotic analysis of series (4.36).

Lemma 4.9. *The following holds true:*

$$N^{2/d}(K - K_N) = \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-\infty:0}) \right] + \sum_{k=-\infty}^{-1} \mathbb{E}_0 \left[\mathcal{H}_{N,k}(Y_{-\infty:0}) - \mathcal{H}_{N,k}(Y_{-\infty:-1}) \right] + o_N(1) \, .$$

Proof. See Appendix F.3. □

As process $(Y_k)_{k \in \mathbb{Z}}$ is stationary, the expectation $\mathbb{E}_0$ enclosed in the sum of the above equation is invariant w.r.t. a time-shift. Using this remark, we obtain after some algebra

$$N^{2/d}(K - K_N) = \lim_{k \to \infty} \mathbb{E}_0 \left[\mathcal{H}_{N,0}(Y_{-\infty:k}) \right] + o_N(1) \, . \tag{4.40}$$

For a fixed $k \geq 0$, (4.7) ensures that sequence $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-m:k}) \right)_{m \geq 0}$ is a Cauchy sequence in $L^1(\mathbb{P}_0)$. Denote its limit by $\ell_k(Y_{-\infty:k})$. The upper bound of (4.8) is uniform in m. Consequently, it also holds for sequence $(\ell_k(Y_{-\infty:k}))_{k \geq 0}$:

$$\mathbb{E}_0 \left\| \ell_k(Y_{-\infty:k}) - \ell_{k-1}(Y_{-\infty:k-1}) \right\| \leq \psi_k \, .$$

Under Assumption 4.4.4, $\sum_k \psi_k$ is a convergent series. Sequence $(\ell_k(Y_{-\infty:k}))_{k\geq 0}$ is thus a Cauchy sequence in $L^1(\mathbb{P}_0)$. Denote its limit by $\ell(Y_{\mathbb{Z}})$. Moreover, the upper bound of (4.7) (resp. (4.8)) is uniform in m' (resp. m). It is then straightforward to prove that $\ell(Y_{\mathbb{Z}})$ coincides with the $L^1(\mathbb{P}_0)$-limit of sequence $\left(\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k})\right)_{k\geq 0}$.

From (4.24) and its counterpart for density p_0, quantity $\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k})$ is uniformly bounded. Consequently, the above limit also holds in the $L^2(\mathbb{P}_0)$-sense:

$$\nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:k}) \xrightarrow[k\to\infty]{L^2(\mathbb{P}_0)} \ell(Y_{\mathbb{Z}}) \,. \tag{4.41}$$

Plugging (4.37) and (4.41) in (4.40) and letting N tend to ∞ complete the proof of Theorem 4.4. □

4.6 Illustration: Case of a hidden Markov process

In this section, we translate our assumptions in the case of (discrete-time) hidden Markov models. For such models, they reduce to simpler conditions on the transition kernel of the underlying Markov chain, and on the observation kernel. This context, where the measurements are noisy samples of a certain Markov source, has raised a deep interest in the recent literature on sensor networks (see [62, 144] and reference therein).

Consider a stationary Markov process $(X_k)_{k\geq 0}$ taking its values in an arbitrary state space X, and playing the role of a source signal to be detected. For each $i \in \{0,1\}$ and each integer t, we assume that the (iterated) transition kernel $\mathbb{P}_i\left[X_{k+t} \in \cdot \,|\, X_k = x\right]$ admits a density $x' \mapsto q_i^t(x,x')$ w.r.t. some probability measure λ on $(\mathsf{X}, B(\mathsf{X}))$. Assume that there exist an integer m, and two real numbers σ^-, σ^+ such that, for each $i \in \{0,1\}$ and each $(x,x') \in \mathsf{X}^2$, $0 < \sigma^- \leq q_i^m(x,x') \leq \sigma^+$. In particular, this assumption implies that the Markov chain $(X_k)_{k\in\mathbb{Z}}$ has bounded support.

If the state space X is finite, the above conditions hold if the Markov chain $(X_k)_{k\in\mathbb{Z}}$ is *irreducible aperiodic*, choosing λ as the (normalized) counting measure on X. In this case, the chain indeed admits a stationary distribution, and $q_i^m(x,x') > 0$ for each x, x' and some integer m [16, Section 8].

The states X_k of the above Markov source are supposed to be hidden. However, a "noisy" version Y_k ($\in \mathsf{Y} \subset \mathbb{R}^d$) of X_k is available at the kth sensor. We assume that the distribution $\mathbb{P}[Y_k \in \cdot\,|X_k = x]$ does not depend on the hypothesis H0 or H1, and admits a density $y \mapsto g(x,y)$ w.r.t. the d-dimensional Lebesgue measure μ restricted to Y, such that $0 < \inf_{x,y} g(x,y) \leq \sup_{x,y} g(x,y) < \infty$. We furthermore assume that this density verifies some smoothness conditions: For each $x \in \mathsf{X}$, $y \mapsto g(x,y)$ is of class C_3 on Y, and $\sup_{\{x\in\mathsf{X},\, y\in\mathsf{Y},\, 1\leq h,i,j\leq d\}} \left|\frac{\partial^3 g}{\partial y^{(h)}\,\partial y^{(i)}\,\partial y^{(j)}}(x,y)\right| < \infty$. The situation is depicted in Figure 4.1.

A similar assumption was recently introduced to study the asymptotic behavior of the log-likelihood $\log p_i(Y_{1:n})$ as n tends to infinity [23, 37]. In particular, it was shown that:

$$|\log p_i(Y_0|Y_{-m:-1}) - \log p_i(Y_0|Y_{-m':-1})| \leq \frac{2}{1-\sigma^-/\sigma^+}\left(\frac{\sigma^-}{\sigma^+}\right)^{m-1} ,$$

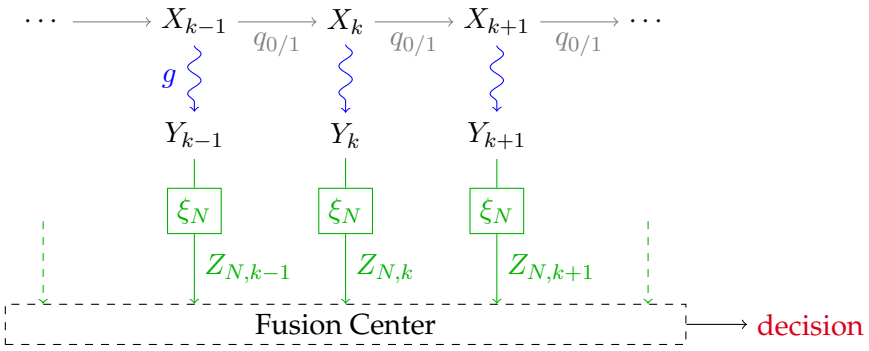


Figure 4.1: Detection of a discrete-time Markov process based on noisy observations.

for each $m' \geq m \geq 0$. This clearly proves that sequence $\log p_i(Y_0|Y_{-m:-1})$ converges in $L^1(\mathbb{P}_0)$ as $m \to \infty$ and yields Assumption 4.2. Moreover, the convergence holds at exponential speed, meaning that quantities $\eta_i(m)$, defined by (4.5), vanish faster than $1/m^6$. The same claim holds as well for quantities $\eta_{i,N}(m)$, without need for any special condition on the quantizer (quantization preserves the hidden Markov nature of the original process $(Y_k)_{k\in\mathbb{Z}}$). This yields Assumption 4.4.3.

Assumptions 4.4.1 and 4.4.2 are direct consequences of the above smoothness conditions on density g. Assumption 4.4.4 can be derived following the arguments of [23, 37]. The following proposition then follows from the results of [23, 37]. The proof is omitted.

Proposition 4.10. *All conditions given by Assumptions 4.1 and 4.4 hold true for the particular process $(Y_k)_{k\in\mathbb{Z}}$ described in this section.*

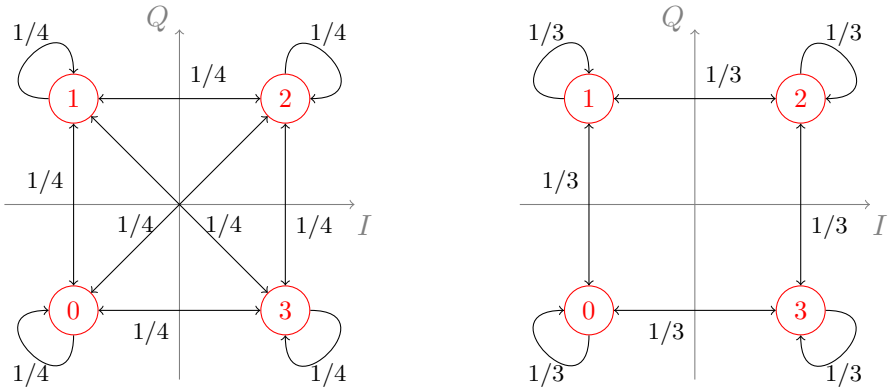
As a consequence, if the family of quantizers moreover verifies Assumption 4.3, then the conclusions of Theorems 4.2 and 4.4 hold true.

Section 4.7.1 below provides a practical example of such a detection problem.

4.7 Numerical results

In this section, we provide numerical illustrations of the proposed quantization rule in terms of geometric properties and performance. Different contexts are considered and we compare several quantizers:

- the *proposed quantizer*, obtained using the approach described in Section 4.4.4.1 and whose model point density is given by (4.15);
- the *MSE-optimal quantizer*, which minimizes $\mathbb{E}_0 \|Y_0 - Z_{N,0}\|^2$ and whose model point density is given by (4.17);
- *Gupta-Hero quantizer*, introduced in [61]: In this case the model point density is drawn as if observations were i.i.d. i.e., only taking the marginal distributions $p_0(y)$ and $p_1(y)$ into account;
- the *uniform quantizer*, with a constant model point density.



(a) QPSK (b) OQPSK

Figure 4.2: QPSK vs. OQPSK–Constellation diagrams and transition probabilities.

4.7.1 Scenario #1: Detection of quaternary modulations: QPSK vs. OQPSK

In this section, we provide an example of hidden Markov models which verify the assumptions given at Section 4.6, and detail how to use in this case the approach described in Section 4.4.4.1 for the design of practical quantizers.

4.7.1.1 Observation model

We consider the following model for vector observations with dimension $d = 2$:

$$Y_k = T(X_k) + W_k \,, \tag{4.42}$$

where $(X_k)_{k\in\mathbb{Z}}$ is a 2-bit message, which takes values in $\mathsf{X} = \{0, 1, 2, 3\}$, $T(x)$ is the 2-D representation of state x in the I-Q plane[5] according to Figure 4.2, and $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, \sigma^2)$ represents a zero mean circular Gaussian thermal noise with variance σ^2. Process $(X_k)_{k\in\mathbb{Z}}$ is i.i.d., uniformly distributed under H0, and forms a Markov chain under H1:

$$\begin{aligned} &\mathsf{H0}: \; X_k \overset{\text{i.i.d.}}{\sim} \mathcal{U}_{\{0,1,2,3\}} \\ &\mathsf{H1}: \; X_0 \sim \mathcal{U}_{\{0,1,2,3\}}, \; \mathbb{P}_1[X_{k+1} = x' | X_k = x] = q(x, x') \,, \end{aligned}$$

where q is the transition matrix of the Markov chain and is given by:

$$q = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \end{bmatrix}.$$

[5] $T(0) = \begin{bmatrix} -1 \\ -1 \end{bmatrix}, T(1) = \begin{bmatrix} -1 \\ 1 \end{bmatrix}, T(2) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, T(3) = \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$

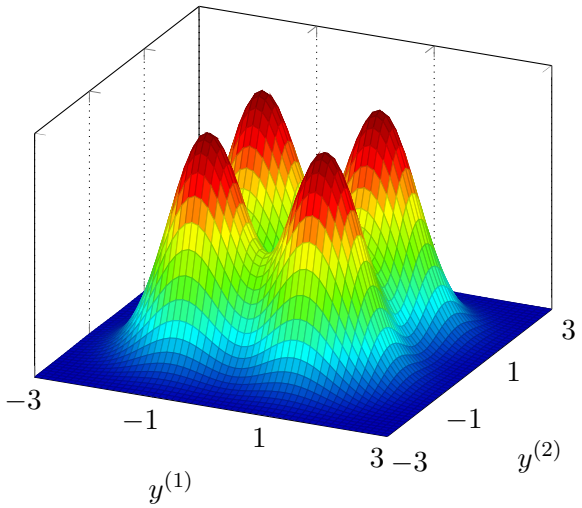


Figure 4.3: QPSK vs. OQPSK–Marginal p.d.f. of the observations $p_0 = p_1$ ($M = 3$, $\sigma = 0.6$).

This situation arises when testing from noisy observations between two possible quaternary modulations, namely quadrature phase-shift keying (QPSK) and offset quadrature phase-shift keying (OQPSK), in the In-phase/Quadrature plane [133, Chapter 3]. The corresponding constellations are depicted in Figure 4.2.

In the observation model (4.42), densities have infinite support. We thus consider truncated observations on $\mathsf{Y} = [-M, M]^2$ for some positive real number M [71, Section 10.1]. The new (truncated) model is a hidden Markov model with observation density $g(x, y)$ given by:

$$g(x,y) = \frac{\mathbf{1}_{[-M,M]^2}(y)}{C_M(\sigma)} \exp\left(\frac{-1}{2\sigma^2}(y - T(x))^{\mathrm{T}}(y - T(x))\right) , \tag{4.43}$$

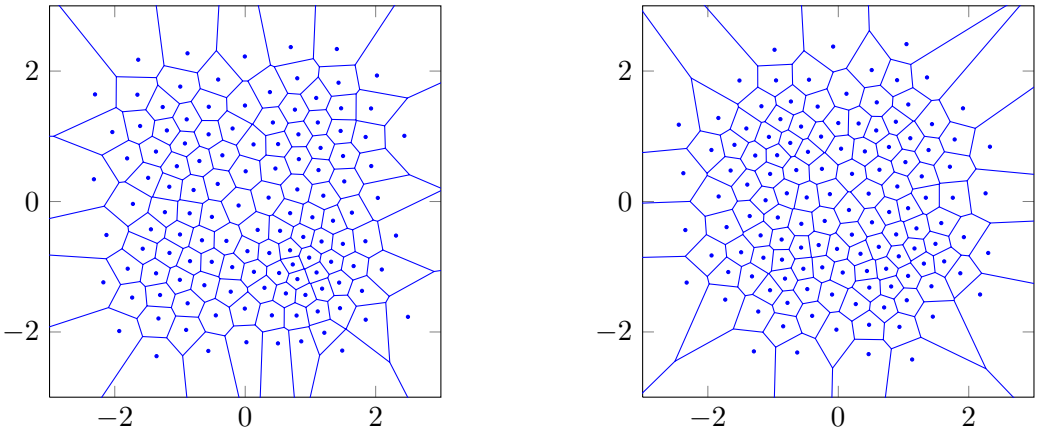
where $\mathbf{1}_A$ stands for the indicator function of set A, and $C_M(\sigma)$ is a constant such that $\int_{\mathsf{Y}} g(x,y)\,\mathrm{d}y = 1$, for each $x \in \{0,1,2,3\}$ i.e., $C_M(\sigma) = \left(\int_{-M}^{M} \exp\left(\frac{-(t-1)^2}{2\sigma^2}\right)\mathrm{d}t\right)^2$.

The above hidden Markov model verifies the assumptions given at Section 4.6. From Proposition 4.10, if the family of quantizers verifies Assumption 4.3, then the conclusions of Theorems 4.2 and 4.4 hold true.

Note that the marginal p.d.f. of the measurements $(Y_k)_{k\geq 0}$ (represented in Figure 4.3) writes

$$p_0(y) = p_1(y) = \frac{1}{4}\sum_{x=0}^{3} g(x,y) . \tag{4.44}$$

Since it does not depend on the hypothesis, Gupta-Hero quantizer [61], which minimizes the error exponent loss in case of i.i.d. observations, is not defined.



(a) MSE-optimal (b) Proposed

Figure 4.4: QPSK vs. OQPSK–128-cell quantizers ($M = 3$, $\sigma = 0.6$, 20 000 samples).

4.7.1.2 Examples of quantizers

Figure 4.4a represents the MSE-optimal 128-cell quantizer obtained by the LBG algorithm, and setting $M = 3$, $\sigma = 0.6$. Figure 4.4b represents the corresponding proposed quantizer. Our quantizer is significantly different from the MSE-optimal one. Some low probability points turn out to be significant for the considered detection problem. Details on how we obtained these quantizers are given below.

MSE-optimal quantizer. The MSE-optimal quantizer of Figure 4.4a was obtained by feeding the LBG algorithm with 20 000 samples following distribution $\mathbb{P}_0$ i.e., i.i.d. with p.d.f. $p_0(y)$ (see Figure 4.3).

Proposed quantizer. As noted in Section 4.4.4.1, the proposed quantizer, whose model point density ζ is given by (4.15), can be obtained by simply feeding the LBG algorithm with observations corresponding with the following p.d.f.:

$$q^*(y) = \frac{p_0(y)\bar{F}(y)}{\int p_0(s)\bar{F}(s)\,\mathrm{d}s}\,.$$

We simulated 20 000 samples of this p.d.f. using rejection sampling [94, Section 2.2]. In practice, we approximated function $\bar{F}$ given by (4.16) by:

$$\bar{F}_k(y) = \frac{1}{n_{MC}} \sum_{j=1}^{n_{MC}} \left\| \nabla_{y_0} \log \frac{p_0}{p_1}(Y_{-k:-1}(j), y, Y_{1:k}(j)) \right\|^2 , \tag{4.45}$$

for $k = 3$ and $n_{MC} = 1\ 000$ replications $(Y_m(j))_{m\in\{-k,\dots,-1,1,\dots,k\},j\in\{1,\dots,n_{MC}\}}$ i.e., 6 000 i.i.d. samples with p.d.f. p_0. These values were chosen based on empirical observations.

The gradient in the above equation may be written as follows, after some derivations, and using (4.43), (4.44):

$$\nabla_{y_0} \log \frac{p_0}{p_1}(y_{-k:k}) = \nabla_{y_0} \log p_0(y_0) - \nabla_{y_0} \log p_1(y_{-k:k})$$
$$= \frac{1}{\sigma^2} \left\{ \frac{\mathbb{E}_0 \left[T(X_0)\, g(X_0, y_0) \right]}{\mathbb{E}_0 \left[g(X_0, y_0) \right]} - \frac{\mathbb{E}_1 \left[T(X_0) \prod_{j=-k}^{k} g(X_j, y_j) \right]}{\mathbb{E}_1 \left[\prod_{j=-k}^{k} g(X_j, y_j) \right]} \right\} .$$

As they are finite sums on X or X^{2k+1}, the above four expectations are exactly computed at the time of the evaluation of $\bar{F}_k$ (4.45).

4.7.2 Scenario #2: Detection of an AR structure in Gaussian 2-D signals

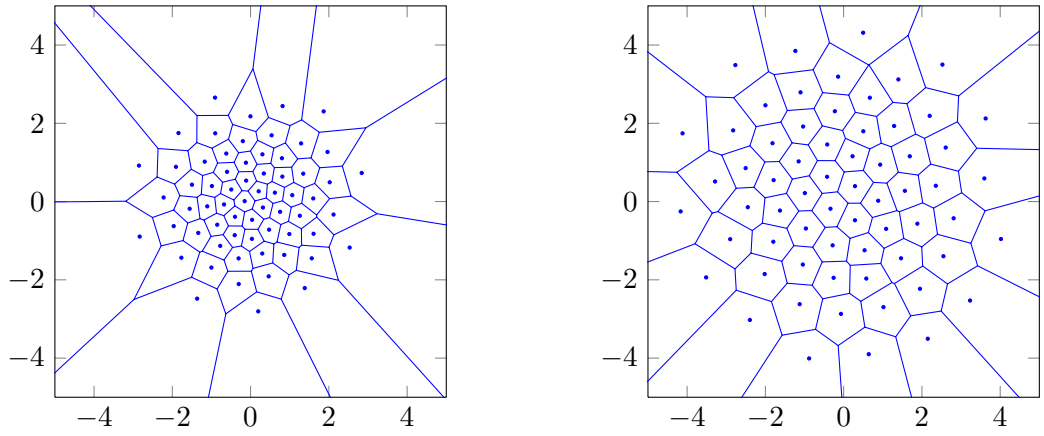
We consider the following model for vector observations with dimension $d = 2$:

$$Y_k = X_k + W_k \ ,$$

where $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, \sigma^2)$ represents a zero mean circular Gaussian thermal noise with variance σ^2, and where $(X_k)_{k \in \mathbb{Z}}$ is a Gaussian process which is white under $\mathsf{H}0$ and correlated (AR-1) under $\mathsf{H}1$. More precisely,

$$\mathsf{H}0 : \ X_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, 1)$$
$$\mathsf{H}1 : \ X_k = a X_{k-1} + \sqrt{1 - a^2}\, U_k \ ,$$

where $a \in (0, 1)$ is the correlation coefficient and $U_k \overset{\text{i.i.d.}}{\sim} \mathcal{CN}(0, 1)$ is the innovation process. In particular, $(Y_k)_{k \in \mathbb{Z}}$ is a white Gaussian process under $\mathsf{H}0$ and is a hidden Markov



(a) MSE-optimal (b) Proposed

Figure 4.5: Detection of an AR structure–64-cell quantizers ($a = 0.8$, $\sigma = 1$, 20 000 samples).

Quantization rule	Uniform on $[-8,8]^2$	MSE-optimal	Proposed
Quantity D_e	8.211	2.255	2.112

Table 4.1: Detection of an AR structure–Quantity D_e ($a = 0.8$, $\sigma = 1$).

process under H1. The marginal distribution of a single observation is identical under both hypotheses.

We mention that in the above model, densities have infinite support so that the assumptions made in this chapter are not satisfied (the observation set Y coincides with $\mathbb{R}^2$ and is thus unbounded). In particular, Theorem 4.4 does not apply. Nevertheless, in order to yield some insights on the design of practical quantizers for detection, we can still use the approach described in Section 4.4.4.1 and compute the proposed model point density given by (4.15).

Figure 4.5a represents the MSE-optimal 64-cell quantizer obtained by the LBG algorithm (with a 20 000-sample training set of data), and setting $\sigma = 1$. Figure 4.5b represents the corresponding proposed quantizer[6], obtained when setting $a = 0.8$. Once again, our quantizer is significantly different from the MSE-optimal one. As a matter of fact, low probability points seem to be significant for the considered detection problem.

Table 4.1 compares the latter two quantization rules and the uniform one (on the rectangle $[-8,8]^2$) in terms of quantity D_e (4.9). As expected, the proposed quantization rule leads to the lowest one. We can guess it will also lead to higher detection performance.

4.7.3 Scenario #3: Detection of a scalar MA process in noise

Denote by Y_k the samples collected by a receiver which makes a binary test associated with the following hypotheses:

$$\begin{aligned} \mathsf{H0}: \; & Y_k = W_k \,, \\ \mathsf{H1}: \; & Y_k = \sum_{\ell=0}^{L} h_\ell \, U_{k-\ell} + W_k \,. \end{aligned}$$

where $W_k \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,\sigma^2)$ represents a thermal noise which is supposed to be real-valued for the sake of illustration. Here, U_k represents a certain random source which is passed through a propagation channel with deterministic real coefficients $h_0,\ldots,h_L$, where L is an integer which represents the channel's memory. In the sequel, we set $L = 3$. Assume for instance that U_k is Gaussian distributed $U_k \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0,1)$. We investigate the case where the sensing unit performs a scalar quantization of the received signal before transmission to the decision device.

As in Section 4.7.2, in the above model, densities have infinite support so that the assumptions made in this chapter are not satisfied. Once again, in order to yield some

[6] In this case, we approximated function $\bar{F}$ (4.16) for finite k and exactly computed the involved expectation.

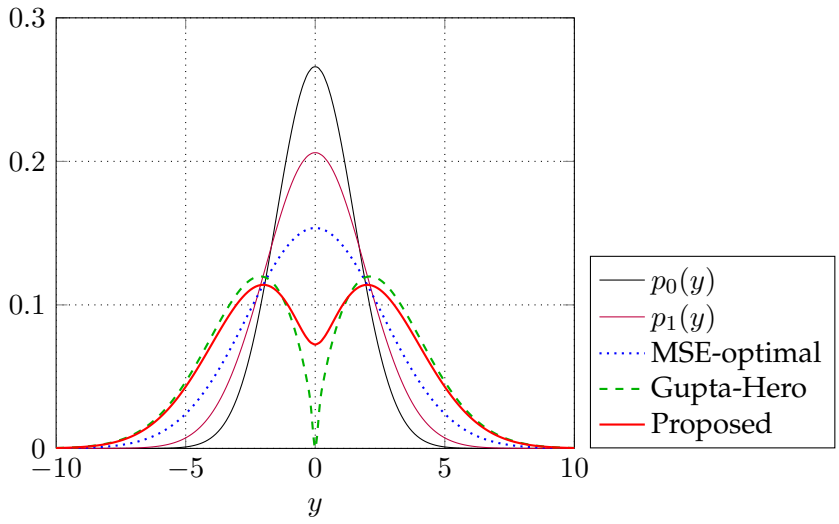


Figure 4.6: Detection of an MA process–Probability and model point densities ($h = [1.06677, -0.59281, 0.09565]$, $\sigma = 1.5$).

insights on the design of practical quantizers for detection, we can still use the approach described in Section 4.4.4.1 and compute the proposed model point density given by (4.15)[7].

For the same reason, the result of Gupta and Hero [61, Eq. (20)] does not apply, but we can compute the corresponding quantizer, which model point density is given by [61, Eq. (25)], as they did for their Gaussian examples in [61, Section V].

The performance depend on the noise variance σ^2 and on the particular value of the channel. Thus, we assumed that channel coefficients $h_0, \ldots, h_L$ are i.i.d. Gaussian distributed with zero mean and unit variance, and made several simulations.

Figure 4.6 represents the probability and model point densities for one channel realization i.e., $h = [1.06677, -0.59281, 0.09565]$, and setting $\sigma = 1.5$.

Considering a system with $n = 80$ sensors, constructing 4-cell quantizers for different methods, and computing the corresponding quantized probability distributions under each hypothesis, we can compare the considered quantization rules in terms of detection performance through their respective receiver operating characteristics (ROC curves). Figure 4.7 represents such curves for the above channel realization. The uniform quantizer is used on the support $[-10\sigma, 10\sigma]$. The whole curve is plotted using $50\,000$ samples of LLR under each hypothesis.

The proposed quantization rule improves the detection performance compared to the MSE-optimal quantizer. In this example, the ROC curve is close to that obtained using Gupta-Hero quantizer. Recall however that in other contexts (e.g., in Scenarios #1 and #2), Gupta-Hero quantizer may not even be defined. We must also qualify this observation:

[7] In this case, we approximated function $\bar{F}$ (4.16) for finite k and exactly computed the involved expectation.

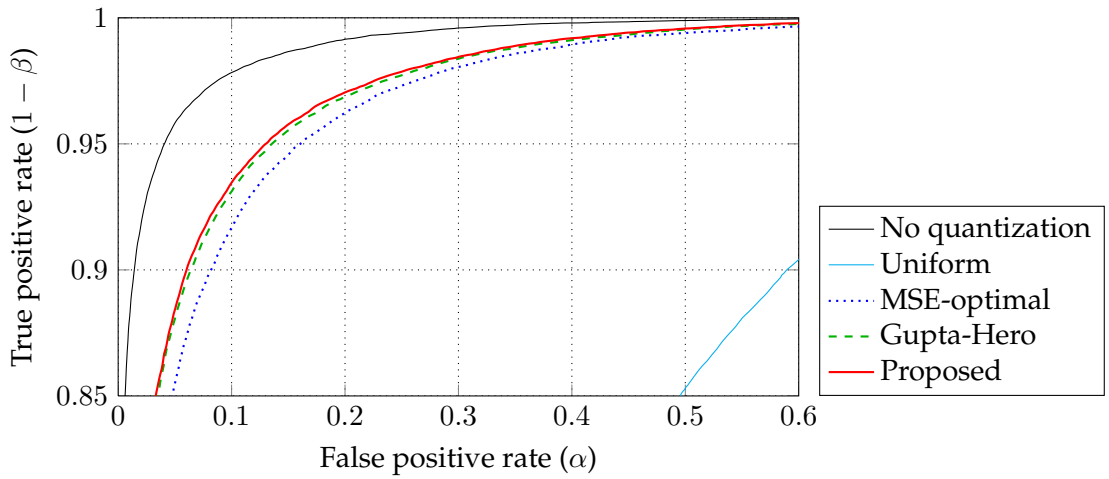


Figure 4.7: Detection of an MA process–ROC curves ($h = [1.06677, -0.59281, 0.09565]$, $\sigma = 1.5$, $n = 80$, $N = 4$, 100 000 samples).

Our theoretical results are valid in the asymptotic regime where N and n tend to infinity, that is, in the regime where the power of the test tends exponentially to one. In practice, the empirical validation of our result would thus require to simulate rare events. This topic is out of the scope of this thesis.

Note that if we interchange H0 and H1, the proposed quantization rule will be different. This is due to the fact that the asymptotic regime we are interested in when dealing with error exponents i.e., n tends to infinity for a fixed type-I error α, restricts attention to one point along the Neyman-Pearson ROC curve.

4.8 Summary

In this chapter, we investigated the performance of the Neyman-Pearson detector used on quantized versions of a correlated vector-valued stationary process. It was shown that for a constant false alarm level, the miss probability of the test converges exponentially to zero. We determined the error exponent, and provided a compact and informative expression of the latter in the context of high-rate quantization. It is proved in particular that when the number N of quantization levels tends to infinity, the error exponent converges at speed $N^{-2/d}$ to the ideal error exponent that one would obtain in the absence of quantization. In case of scalar quantization, we analytically characterized the high-rate quantizers minimizing the error exponent loss. In case of vector quantization, we proposed a method based on the LBG algorithm in order to construct practical quantizers with attractive performance.

These detection-oriented quantization strategies aim at improving the detection performance for a given rate. Alternatively, the lowest number of bits necessary to achieve some given performance can be studied. The proposed quantizers should help to reduce

the resource needs of detection systems.

We believe that there are many directions for extending these results and mention a few here. In this chapter, observations have absolutely continuous probability distributions w.r.t. the Lebesgue measure. Following Graf and Luschgy [53, Section 6] who considered measures with both continuous and singular parts, we could think of an extension of our work to such cases. We moreover focused on constant false-alarm rate (CFAR) tests. Following the arguments developed in [7, 61] and using the results of [27, Section III], it could be interesting to study the whole asymptotic ROC curve and use a global performance criterion like the area under the curve (AUC). However, this would require a nontrivial extension of Sanov's theorem [35] to non-i.i.d. times series.

CHAPTER 5

Conclusion

5.1 General comments

In this thesis, we derived some fundamental results on coding for secure transmission of sources with side information (in Chapters 2 and 3), and coding for detection (in Chapter 4). In particular, Chapters 2 and 3 provided several new results of optimality i.e., single-letter characterizations of achievable regions. It was shown in these cases how to use potential advantages –in terms of side information and/or channel– of the legitimate user to maximize secrecy against an eavesdropper. Chapter 4 gave weak conditions for the convergence of the error exponent of the Neyman-Pearson test performed on quantized observations in the high-rate regime, and the corresponding speed as well. We believe that these results and the corresponding techniques can be used to study several other problems, as detailed in the following sections.

The main limitations of our results essentially come from the fact that they include some well-known long-standing open problems. For instance, the general setting of multiterminal secure source coding considered in Chapter 2 can be seen as an extension of the Berger-Tung problem taking security requirements into account. The original Berger-Tung problem remains open i.e., best known results only provide inner and outer bounds that do not match in general. The same applies in the considered secure setting.

Chapter 3 investigated the more general problem of secure transmission of sources over noisy channels. As a matter of fact, even if the intuition indicates that separation would hold, it is still not clear if this is always true. We indeed derived several results of separation but also proposed a hybrid digital/analog scheme that is optimal in a Gaussian example, letting the general case open.

In Chapter 4, knowing the asymptotic expression of the loss in error exponent due to quantization was not sufficient to design the best quantization strategy in the vector case. The final expression indeed involves the model covariation profile, an asymptotic quantity that captures the shape of cells of vector quantizers in the high-rate regime. The set of all admissible such matrices is unfortunately still unknown [54] so that we can only provide locally optimal quantizers (in some given sub-classes).

In spite of the aforementioned limitations, several possible extensions of this work can be identified, as detailed below.

5.2 Further directions for secure transmission

First of all, the results of Chapter 2 have already inspired some new results. In a recent paper [41], region $\mathcal{R}^*_{\text{uncoded}}$ was studied for a vector Gaussian source with vector Gaussian side informations. From the single-letter characterization of Theorem 2.6, the authors derived an outer bound on the achievable rate R and leakage rate I_e, for some fixed distortion level D. This outer bound was furthermore proved to be tight at the limit $R \to \infty$, providing the minimal leakage rate $I_e^{\min}(D)$ when the legitimate user needs to reconstruct the source within a prescribed distortion level D.

Following recent work on *source coding with a side information vending machine* [126], an extension of Theorem 2.6 to action-dependent side information was also proposed [77]. In this setting, as depicted in Figure 5.1, an action sequence T^n is generated based on the rate-limited message J with some cost $\Lambda(T^n)$ to influence the side information at both receivers. For instance, in a "switch on/off" setup, Bob can observe his side information if and only if some constant cost is paid. In general, Alice wishes to simultaneously guarantee a distortion level at Bob D, an average cost P, and an equivocation rate at Eve Δ. A single-letter characterization of the set of all achievable tuples (R_A, D, P, Δ), referred to as the *rate-distortion-cost-equivocation region* and denoted by $\mathcal{R}^*_{\text{action}}$, was derived:

Theorem 5.1 (Secure source coding with action-dependent side information [77])**.** *Region $\mathcal{R}^*_{action}$ writes as the set of all tuples $(R_A, D, P, \Delta) \in \mathbb{R}^4_+$ such that there exist random variables U, V, T on $\mathcal{U}$, $\mathcal{V}$, $\mathcal{T}$, respectively, with joint distribution $p(uvatce) = p(u|v)p(v|at)p(t|a)p(a)$ $p(ce|at)$, and a function $\hat{A}\colon \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, verifying the following inequalities:*

$$
\begin{aligned}
R_A &\geq I(T;A) + I(V;A|CT)\,, \\
D &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\,, \\
P &\geq \mathbb{E}\big[\Lambda(T)\big]\,, \\
\Delta &\leq H(A|VCT) + I(A;C|UT) - I(A;E|UT)\,.
\end{aligned}
$$

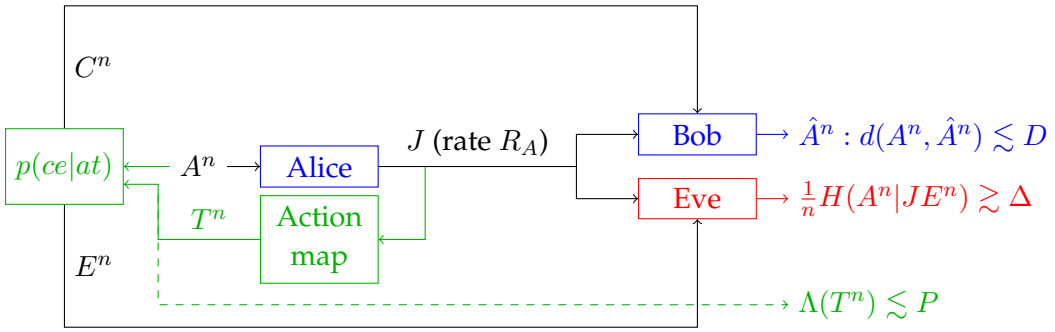


Figure 5.1: Secure source coding with action-dependent side information [77].

From the results of Chapter 2, we can also think about an extension of the CEO problem [13, 43] with some additional security constraints. In the classical CEO problem, L agents observe noisy versions $\{T_{[\ell]}\}_{\ell\in\{1,\dots,L\}}$ of a common hidden random variable S. They can communicate compressed versions of their observations to the Chief Executive Officer (CEO) through rate-limited links with respective rates $\{R_\ell\}_{\ell\in\{1,\dots,L\}}$. From the received messages, the CEO wants to eventually find an estimate $\hat{S}$ of S within a certain distortion level D. This general CEO problem is still open i.e., an exact characterization of the achievable rates and distortion level is not known. When $L = 2$, the quadratic Gaussian case[1] has however been solved [121]. The quadratic Gaussian case has also been solved if the quantity of interest is the sum-rate $\sum_{\ell=1}^{L} R_\ell$ only, and if L is not constrained ($L \to \infty$) [120].

Extensions of these settings to take security requirement into account could be performed assuming that one agent, say number L, is corrupted. This untrusted agent observes $T_{[L]}$ and has also access to some (say K) links between other agents and the CEO, as depicted in Figure 5.2. The security of the system is measured through the equivocation about S at this eavesdropper. There is obviously a trade-off between the quantities of interest: Reducing the distortion level at the CEO imposes to transmit better descriptions, which may result in sending more information on the eavesdropped links. In the following paragraphs, we give a formal definition of this problem.

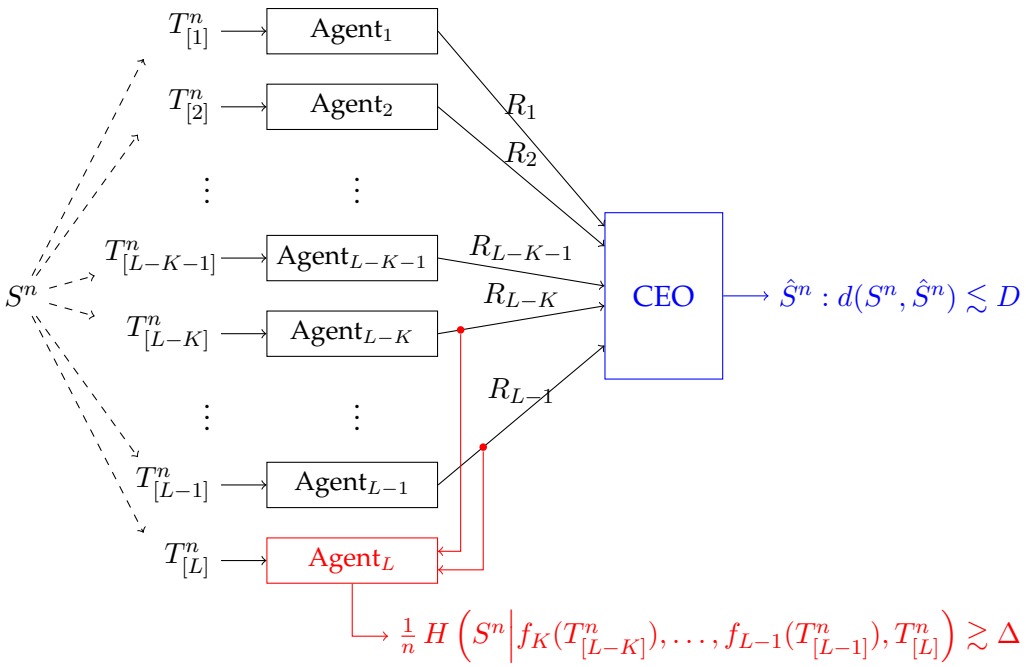


Figure 5.2: CEO problem with security requirement.

[1]The hidden source S is Gaussian; the observations $\{T_{[\ell]}\}_{\ell\in\{1,\dots,L\}}$ are the outputs of independent AWGN channels with input S; the distortion measure is the Euclidean distance on $\mathbb{R}$.

Let $\mathcal{S}$, $\mathcal{T}$ be two finite sets, and $K \leq L \in \mathbb{N}^*$. The hidden source sequence $(S_i)_{i\in\mathbb{N}^*}$ is i.i.d. distributed with probability distribution $p(s)$ on $\mathcal{S}$. For any $\ell \in \{1,\dots,L\}$, agent ℓ observes the sequence of random variables $(T_{[\ell],i})_{i\in\mathbb{N}^*}$, which take values on $\mathcal{T}$; for each $i \in \mathbb{N}^*$, random variable $T_{[\ell],i}$ only depends on the source S_i, according to the transition probability $p(t|s)$.

Let $d\colon \mathcal{A}\times\mathcal{A} \to [0, d_{\max}]$ be a finite distortion measure i.e., such that $0 \leq d_{\max} < \infty$. We also denote by d the component-wise mean distortion on $\mathcal{A}^n \times \mathcal{A}^n$.

Definition 5.1 (Code)**.** An (n, L, R)-code for source coding in this setup is defined by

- $L-1$ encoding functions $f_\ell\colon \mathcal{T}^n \to \{1,\dots,2^{nR_\ell}\}$, where the rates $\{R_\ell\}_{\ell\in\{1,\dots,L-1\}}$ are such that $\sum_{\ell=1}^{L-1} R_\ell = R$,
- a decoding function at the CEO $g\colon \{1,\dots,2^{nR_1}\}\times\cdots\times\{1,\dots,2^{nR_{L-1}}\} \to \mathcal{S}^n$.

Definition 5.2 ((K,L)-achievability)**.** A tuple $(R, D, \Delta) \in \mathbb{R}_+^3$ is said to be (K, L)-*achievable* if, for any $\varepsilon > 0$, there exists an $(n, L, R+\varepsilon)$-code $(f_1,\dots,f_{L-1}, g)$ such that:

$$\mathbb{E}\left[d\left(S^n, g\big(f_1(T^n_{[1]}),\dots,f_{L-1}(T^n_{[L-1]})\big)\right)\right] \leq D+\varepsilon\,,$$
$$\frac{1}{n}H\left(S^n\middle|f_K(T^n_{[L-K]}),\dots,f_{L-1}(T^n_{[L-1]}),T^n_{[L]}\right) \geq \Delta-\varepsilon\,.$$

Similarly to [13, 120], since we are only interested in the sum-rate, we can let L tend to infinity. The eavesdropper should then observe a constant *fraction* α of the L links i.e., K should also tend to infinity such that $K \simeq \alpha L$:

Definition 5.3 (Achievability)**.** A tuple (α, R, D, Δ) is said to be *achievable* if (R, D, Δ) is (K, L)-achievable for some $K \leq L \in \mathbb{N}^*$ such that $\frac{K}{L} \geq \alpha$.

Recent results [26] indicate that Wyner-Ziv-like coding works well in a classical CEO setup. Since the coding schemes proposed in this thesis rely on random binning and properties of typical sequences, it is wise to think that similar schemes could be used in the above secure setting.

More generally, we believe that the framework developed in Chapters 2 and 3 can be applied to communication settings with many sources and channels (e.g., relay channel, MAC). In particular, further extensions could include the introduction of multiple eavesdroppers. In a *compound* approach, this enables to consider the fact that the encoder has an imperfect knowledge of the statistics of the side information and the channel of the eavesdropper. As a matter of fact, if the observations of these multiple eavesdroppers are degraded, as it will always be the case with scalar Gaussian variables, then a multi-layer superposition coding scheme may yield a characterization of the equivocation rate at each eavesdropper.

Besides the above settings related to communication systems, similar security requirements while compressing a source also appear in other contexts. For instance, managers of *databases* (containing medical data, customer preferences, social-network graphs, etc.) would like to publicize some entries while ensuring the privacy of the subjects. This

usually occurs in order to conduct statistical studies on the cohort for e.g., public health or social surveys. To prevent from relating the information and real people, databases are currently *anonymized* (or *de-identified* i.e., the name and some other sensitive data are simply erased). This procedure is however highly insecure as other information might be publicly available, enabling mitigation and eventual re-identification [114, 115]. To handle such situation, a general framework for *privacy and utility in databases* has been proposed recently [137]. As a matter of fact, if this problem and the one of secure source coding are quite different, it is shown that they are somehow related [137, Theorem 1]. Theoretical results on such security/privacy problems now appear to be essential as the amount of processed, stored, and shared personal data increases (through e.g., social networks, smartphones, or smart electrical meters).

5.3 Further directions for high-rate quantization

We think that the framework developed in Chapter 4 for detection-oriented high-rate quantization of correlated processes can be applied in other contexts. For instance, parameter estimation problems could be studied through the asymptotic behavior of the Fisher information, which yields a lower bound on the variance of any estimator, due to the Cramér-Rao lower bound [75]. If the observations are scalar and i.i.d., [129, Section III-C] provides the asymptotic loss in terms of Fisher information due to uniform quantization in the high-rate regime. Denoting by p_θ the probability density of the observations $(Y_k)_{k\in\mathbb{N}}$ with (unknown, fixed) parameter $\theta \in \mathbb{R}$, and $\hat{\theta}_{N,n}$ the maximum-likelihood estimator of θ based on n samples $Y_{1:n} = (Y_1, \dots, Y_n)$ uniformly quantized on N levels, this result roughly gives the following approximation for large n and N:

$$\mathbb{E}\left[\left(\hat{\theta}_{N,n} - \theta\right)^2\right] \approx \frac{1}{n\,\mathbb{E}\left[(\psi_\theta(Y_0))^2\right]} \left(1 + \frac{1}{12N^2} \frac{\mathbb{E}\left[(\psi'_\theta(Y_0))^2\right]}{\mathbb{E}\left[(\psi_\theta(Y_0))^2\right]}\right), \tag{5.1}$$

where $\psi_\theta(y) = \frac{\partial}{\partial\theta} \log p_\theta(y)$ is the so-called *score function*, and $\psi'_\theta(y) = \frac{\partial}{\partial y}\psi_\theta(y)$.

Some on-going work [15] aims at investigating adaptive quantization for statistical inference (as depicted in Figure 5.3), first extending the above approximation to recursive *on-line* estimators of *vector* parameters from *vector*-valued i.i.d. processes. In the following paragraphs, we give some basic definitions of this problem, as well as primary results.

Let $(Y_k)_{k\in\mathbb{N}}$ be an i.i.d. random process on some bounded convex subset Y of $\mathbb{R}^m$ with probability density p_θ for some fixed, unknown $\theta \in \Theta$, where Θ is a compact convex subset of $\mathbb{R}^d$. Quantizer $(\mathcal{C}_N, \Xi_N, \xi_N)$ is defined as in Section 4.3.1. Quantity $Z_{N,k} = \xi_N(Y_k)$ denotes the k-th measurement quantized on $\log_2(N)$ bits. For each quantization point $\xi_{N,j}$,

$$p_{\theta,N}(\xi_{N,j}) = \int_{C_{N,j}} p_\theta(y)\,\mathrm{d}y$$

is the probability that random variable Y_0 falls into the cell $C_{N,j}$ associated with the observed point $\xi_{N,j}$.

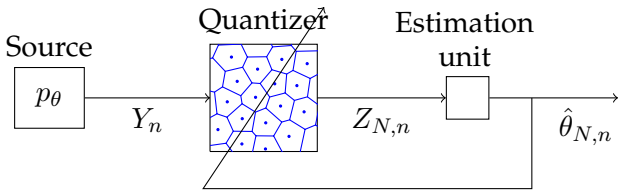


Figure 5.3: Adaptive quantization for parameter estimation [15].

Assuming that the quantizer is known at the decision device, the aim is to find an estimate $\hat{\theta}$ of θ based on the observation of $Z_{N,1:n}$ i.e., to search for $p_{\hat{\theta},N}$ that best fits (in a maximum likelihood sense) the quantized data $Z_{N,1:n}$. Focusing on recursive estimation –one estimate $\theta_{N,k+1}$ is generated at each time instant $k+1$ based on the most recent observation $Z_{N,k+1}$ and the past estimate $\theta_{N,k}$, the idea is to use a stochastic gradient descent of the form:

$$\theta_{N,k+1} = \theta_{N,k} + \gamma_k \, \nabla_\theta \log p_{\theta_{N,k}}(Z_{N,k+1})$$

for any $k \geq 0$, where ∇_θ represents the gradient operator w.r.t. θ, and $\gamma_k > 0$ is a deterministic step size. Polyak averaging [82] is then performed to obtain the final estimate defined as

$$\hat{\theta}_{N,n} = \frac{1}{n} \sum_{k=1}^{n} \theta_{N,k} \; .$$

Under some conditions on the densities $(p_\theta)_{\theta \in \Theta}$, the step size sequence $(\gamma_k)_{k \in \mathbb{N}^*}$, and the quantizer, it can be shown that

$$n \, \mathbb{E}\left[\left\| \hat{\theta}_{N,n} - \theta \right\|^2 \right] \xrightarrow[n \to \infty]{} \mathrm{Tr}\left(J_N^{-1} \right) \; ,$$

where J_N is the so-called *Fisher information matrix* [86] of $Z_{N,0}$.

In the *high-rate* regime, using the notation of Chapter 4, the following approximation holds for large n, N (see Theorem 5.2 below):

$$\mathbb{E}\left[\left\| \hat{\theta}_{N,n} - \theta \right\|^2 \right] \approx \frac{1}{n} \left(\mathrm{Tr}\left(J^{-1} \right) + \frac{1}{N^{2/d}} \, \mathbb{E}\left[\frac{\mathrm{Tr}\left(J^{-2} \, \Psi'_\theta(Y_0)^{\mathrm{T}} M(Y_0) \Psi'_\theta(Y_0) \right)}{\zeta(Y_0)^{2/d}} \right] \right) \; , \tag{5.2}$$

where $J = \mathbb{E}\left[\Psi_\theta(Y_0) \Psi_\theta(Y_0)^{\mathrm{T}} \right]$ is the Fisher information matrix of Y_0 (that one would obtain in the absence of quantization), $\Psi_\theta(y) = \nabla_\theta \log p_\theta(y)$, and $\Psi'_\theta(y) = \nabla_y \Psi_\theta(y)^{\mathrm{T}}$. The expectation in the r.h.s. of the above equation corresponds to the *asymptotic MSE loss due to quantization*, and will be denoted by D_m. Note that (5.2) includes (5.1) as a special case for $m = d = 1$, and $M(y) = 1/12$.

Theorem 5.2 (Asymptotic Fisher information loss [15])**.** *Under Assumption 4.3 and some conditions on the densities* $(p_\theta)_{\theta \in \Theta}$*,*

$$N^{2/d}(J - J_N) \xrightarrow[N \to \infty]{} \int \frac{\Psi_\theta(y)^{\mathrm{T}} M(y) \Psi_\theta(y)}{\zeta(y)^{2/d}} \, p_\theta(y) \, \mathrm{d}y \; .$$

The above expression resembles (4.9) and [61, Eq. (20)]. Similarly, it only depends on the quantizer through its asymptotic characteristics, the model point density ζ and the model covariation profile M. Comments of Sections 4.4.3 and 4.4.4 thus also apply here. In particular, focusing on congruent cells with minimum moment of inertia i.e., s.t. $M(y) = \nu I_m$, Hölder's inequality yields

$$D_m \geq \nu \left(\int \left[\left\| J^{-1} \Psi_\theta(y) \right\|_F^2 p_\theta(y) \right]^{\frac{d}{d+2}} \mathrm{d}y \right)^{\frac{d+2}{d}} , \tag{5.3}$$

where $\|\cdot\|_F$ denotes the Frobenius matrix norm. Equality is achieved in the above equation when

$$\zeta(y) = \frac{\left[\left\| J^{-1} \Psi_\theta(y) \right\|_F^2 p_\theta(y) \right]^{\frac{d}{d+2}}}{\int \left[\left\| J^{-1} \Psi_\theta(s) \right\|_F^2 p_\theta(s) \right]^{\frac{d}{d+2}} \mathrm{d}s} .$$

As expected, this optimal model point density depends on the *true* distribution p_θ, which is of course unknown in the framework of parameter estimation. The idea is then to learn the desired quantizer ζ with a recursive procedure at the same time as the estimation of θ (see Figure 5.3). In [168], Kohonen's algorithm has been adapted for *learning vector quantization*. The proposed algorithm recursively generates (from a training set of data) a Voronoi tessellation that asymptotically minimizes the MSE for some p.d.f.. Controlling the step sizes of the two simultaneous recursive equations (that update the estimate and the quantizer), it is expected that the asymptotic MSE loss due to quantization is still given by (5.3) [15].

Following the arguments of the above paragraphs, and of Chapter 4, one could further prove an approximation similar to (5.2) for parameter estimation with *correlated* observations, under some mixing conditions (as the ones of Assumption 4.4).

In both detection and parameter estimation settings, the quantities of interest are of the form "$\mathbb{E}[\log p]$" for some probability density p. In fact, the technique used in this thesis could apply to other settings in statistical inference as long as it involves such quantities e.g., order estimation of finite-state hidden Markov models [23, 46]. Moreover, the generalized f-divergence and the corresponding loss due to uniform scalar quantization were investigated in [129]. It yields results that apply to binary hypothesis testing (through e.g., Kullback-Leibler divergence [81], Bhattacharyya distance [14]), to data estimation (through mean square error), and to parameter estimation (through Fisher information, as detailed in the above paragraphs), for scalar i.i.d. processes. Extensions to *correlated vector*-valued processes of this generalized f-divergence, and associated results on high-rate quantization, seem inspiring, as well as promising in terms of practical applications.

Part III

Annexes

–

Appendices

Table of Contents

APPENDIX A

Strongly Typical Sequences and Delta-Convention

Following [34], we use in this dissertation *strongly typical sets* and the so-called *Delta-Convention*. Some useful facts are recalled here. Let X and Y be random variables on some finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. We denote by $p_{X,Y}$ (resp. $p_{Y|X}$, and p_X) the joint probability distribution of (X,Y) (resp. conditional distribution of Y given X, and marginal distribution of X).

Definition A.1 (Number of occurrences)**.** For any sequence $x^n \in \mathcal{X}^n$ and any symbol $a \in \mathcal{X}$, notation $N(a|x^n)$ stands for the number of occurrences of a in x^n.

Definition A.2 (Typical sequence)**.** A sequence $x^n \in \mathcal{X}^n$ is called *(strongly) δ-typical* w.r.t. X (or simply *typical* if the context is clear) if

$$\left|\frac{1}{n}N(a|x^n) - p_X(a)\right| \leq \delta \text{ for each } a \in \mathcal{X} ,$$

and $N(a|x^n) = 0$ for each $a \in \mathcal{X}$ such that $p_X(a) = 0$. The set of all such sequences is denoted by $T^n_\delta(X)$.

Definition A.3 (Conditionally typical sequence)**.** Let $x^n \in \mathcal{X}^n$. A sequence $y^n \in \mathcal{Y}^n$ is called *(strongly) δ-typical (w.r.t. Y) given x^n* if

$$\left|\frac{1}{n}N(a,b|x^n,y^n) - \frac{1}{n}N(a|x^n)p_{Y|X}(b|a)\right| \leq \delta \text{ for each } a \in \mathcal{X}, b \in \mathcal{Y} ,$$

and, $N(a,b|x^n,y^n) = 0$ for each $a \in \mathcal{X}$, $b \in \mathcal{Y}$ such that $p_{Y|X}(b|a) = 0$. The set of all such sequences is denoted by $T^n_\delta(Y|x^n)$.

Delta-Convention [34]. For any sets $\mathcal{X}$, $\mathcal{Y}$, there exists a sequence $\{\delta_n\}_{n\in\mathbb{N}^*}$ such that the lemmas stated below hold.[1] From now on, typical sequences are understood with $\delta = \delta_n$. Typical sets are still denoted by $T^n_\delta(\cdot)$.

Lemma A.1 ([34, Lemma 1.2.12])**.** *There exists a sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ such that*

$$p_X(T^n_\delta(X)) \geq 1 - \eta_n .$$

[1] As a matter of fact, $\delta_n \to 0$ and $\sqrt{n}\,\delta_n \to \infty$ as $n \to \infty$.

Lemma A.2 ([34, Lemma 1.2.13]). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$,

$$\left|\frac{1}{n}\log\|T_\delta^n(X)\| - H(X)\right| \leq \eta_n \,,$$
$$\left|\frac{1}{n}\log\|T_\delta^n(Y|x^n)\| - H(Y|X)\right| \leq \eta_n \,.$$

Lemma A.3 (Asymptotic equipartition property). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$ *and each* $y^n \in T_\delta^n(Y|x^n)$,

$$\left|-\frac{1}{n}\log p_X(x^n) - H(X)\right| \leq \eta_n \,,$$
$$\left|-\frac{1}{n}\log p_{Y|X}(y^n|x^n) - H(Y|X)\right| \leq \eta_n \,.$$

Lemma A.4 (Joint typicality lemma [42]). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that*

$$\left|-\frac{1}{n}\log p_Y(T_\delta^n(Y|x^n)) - I(X;Y)\right| \leq \eta_n \text{ for each } x^n \in T_\delta^n(X) \,.$$

Proof.

$$\begin{aligned} p_Y(T_\delta^n(Y|x^n)) &= \sum_{y^n \in T_\delta^n(Y|x^n)} p_Y(y^n) \\ &\overset{(a)}{\leq} \|T_\delta^n(Y|x^n)\|\; 2^{-n[H(Y)-\alpha_n]} \\ &\overset{(b)}{\leq} 2^{n[H(Y|X)+\beta_n]}\, 2^{-n[H(Y)-\alpha_n]} \\ &= 2^{-n[I(X;Y)-\beta_n-\alpha_n]} \,, \end{aligned}$$

where

- step (a) follows from the fact that $T_\delta^n(Y|x^n) \subset T_\delta^n(Y)$ and Lemma A.3, for some sequence $\alpha_n \xrightarrow[n\to\infty]{} 0$,
- step (b) from Lemma A.2, for some sequence $\beta_n \xrightarrow[n\to\infty]{} 0$.

The reverse inequality $p_Y(T_\delta^n(Y|x^n)) \geq 2^{-n[I(X;Y)+\beta_n+\alpha_n]}$ can be proved following similar argument. □

APPENDIX B

Graphical Representation of Probability Distributions

Following [127, Section II], we use in this dissertation a technique based on undirected graphs, that provides a sufficient condition for establishing Markov chains from a joint distribution. Such a technique for establishing conditional independence was introduced in [123] for Bayesian networks, and further generalized to various types of graphs [80]. This paragraph recalls the main points of this technique.

Assume that a sequence of random variables X^n has joint distribution with the following form:

$$p(x^n) = f_1(x_{\mathcal{S}_1}) f_2(x_{\mathcal{S}_2}) \cdots f_k(x_{\mathcal{S}_k}) \,,$$

where, for each $i \in \{1, \ldots, k\}$, $\mathcal{S}_i$ is a subset of $\{1, \ldots, n\}$, notation $x_{\mathcal{S}_i}$ stands for collection $(x_j)_{j \in \mathcal{S}_i}$, and f_i is some nonnegative function.

B.1 Drawing the graph

Draw an undirected graph where all involved random variables e.g., $(X_j)_{j \in \{1,\ldots,n\}}$, are nodes. For each $i \in \{1, \ldots, k\}$, draw edges between all the nodes in $X_{\mathcal{S}_i}$.

B.2 Checking Markov relations

Let $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ be three disjoint subsets of $\{1, \ldots, n\}$. If all paths in the graph from a node in $X_{\mathcal{G}_1}$ to a node in $X_{\mathcal{G}_3}$ pass through a node in $X_{\mathcal{G}_2}$, then $X_{\mathcal{G}_1} \multimap X_{\mathcal{G}_2} \multimap X_{\mathcal{G}_3}$ form a Markov chain. The proof of this result can be found in [127] and is omitted here.

APPENDIX C

Useful Information-Theoretic Lemmas

C.1 Csiszár and Körner's equality

The following lemma can be found in [32, Lemma 7].

Lemma C.1 (Csiszár and Körner's equality)**.** *Consider two i.i.d. sequences X^n and Y^n, and a constant C. The following identity holds true:*

$$\sum_{i=1}^{n} I(Y_{i+1}^n; X_i | C X^{i-1}) = \sum_{j=1}^{n} I(X^{j-1}; Y_j | C Y_{j+1}^n) \, .$$

Proof. From the chain rule for conditional mutual information, we can write:

$$\begin{aligned}
\sum_{i=1}^{n} I(Y_{i+1}^n; X_i | C X^{i-1}) &= \sum_{i=1}^{n} \sum_{j=i+1}^{n} I(Y_j; X_i | C X^{i-1} Y_{j+1}^n) \\
&= \sum_{i,j:\, i<j} I(Y_j; X_i | C X^{i-1} Y_{j+1}^n) \\
&= \sum_{j=1}^{n} \sum_{i=1}^{j-1} I(X_i; Y_j | C X^{i-1} Y_{j+1}^n) \\
&= \sum_{j=1}^{n} I(X^{j-1}; Y_j | C Y_{j+1}^n) \, .
\end{aligned}$$

□

C.2 Mrs. Gerber's lemma

The following lemma can be found in [164].

Lemma C.2 (Mrs. Gerber's Lemma)**.** *Let X be a binary random variable, and Y be the output of a binary symmetric channel with crossover probability $\epsilon \in [0, \frac{1}{2}]$ and input X. Then,*

$$H(Y) = h_2 \left(\epsilon \star h_2^{-1}\big(H(X)\big) \right) \, .$$

The following corollary directly follows from Lemma C.2 together with Jensen's inequality.

Corollary C.3. *Let X and Y be defined as in Lemma C.2, and U be an arbitrary random variable on some finite set $\mathcal{U}$ such that $U \multimap X \multimap Y$ form a Markov chain. Then,*

$$H(Y|U) \geq h_2\left(\epsilon \star h_2^{-1}\big(H(X|U)\big)\right) .$$

Proof. The conditional entropy of Y given U writes

$$H(Y|U) = \sum_{u\in\mathcal{U}} H(Y|U=u)p(u) .$$

Then, for each $u \in \mathcal{U}$, given the event $\{U = u\}$, Y is the output of a BSC with crossover probability $\epsilon \in [0, \frac{1}{2}]$ and input $X \sim p_{X|U=u}$. Lemma C.2 applies:

$$H(Y|U=u) = h_2\left(\epsilon \star h_2^{-1}\big(H(X|U=u)\big)\right) .$$

Gathering the two above equations yields:

$$\begin{aligned} H(Y|U) &= \sum_{u\in\mathcal{U}} h_2\left(\epsilon \star h_2^{-1}\big(H(X|U=u)\big)\right) p(u) \\ &\geq h_2\left(\epsilon \star h_2^{-1}\left(\sum_{u\in\mathcal{U}} H(X|U=u)p(u)\right)\right) \\ &= h_2\left(\epsilon \star h_2^{-1}\big(H(X|U)\big)\right) , \end{aligned}$$

where the lower bound follows from the fact that function $x \mapsto h_2\left(\epsilon \star h_2^{-1}(x)\right)$ is convex [164, Lemma 2] and Jensen's inequality. □

C.3 Entropy power inequality

The following lemmas can be found in [139], [42].

Lemma C.4 (EPI)**.** *If X^n and Y^n are independent random vectors with densities, then*

$$2^{\frac{2}{n}h(X^n+Y^n)} \geq 2^{\frac{2}{n}h(X^n)} + 2^{\frac{2}{n}h(Y^n)} .$$

Lemma C.5 (Conditional EPI)**.** *Let U be an arbitrary random variable. If X^n and Y^n are random vectors verifying the Markov chain $X^n \multimap U \multimap Y^n$ (with conditional densities), then*

$$2^{\frac{2}{n}h(X^n+Y^n|U)} \geq 2^{\frac{2}{n}h(X^n|U)} + 2^{\frac{2}{n}h(Y^n|U)} .$$

APPENDIX D

Auxiliary Proofs of Chapter 2

D.1 Proof of Lemma 2.4

In this section, we study each term of the r.h.s. of (2.7) and prove Lemma 2.4 using the joint typicality lemma (see Appendix A).

D.1.1 Proof of (2.8)

The probability that Bob fails to decode index s writes:

$$\begin{aligned}
\Pr\{\not{s}\} &= \Pr\Big\{\exists\, s_1', s_2', s' \neq s \text{ s.t. } (u^n(s_1'), v^n(s_1', s_2'), w^n(s')) \\
&\qquad\qquad \in (B_1(r_1) \times B_2(s_1', r_2) \times B_C(r)) \cap T_\delta^n(U,V,W)\Big\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon)} \\
&\qquad \times \Pr\Big\{(U^n, V^n, W^n) \in T_\delta^n(U,V,W) \,\Big|\, (U^n, V^n) \in T_\delta^n(U,V), W^n \in T_\delta^n(W)\Big\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon)}\, 2^{-n(I(UV;W) - \eta_n)} \\
&= 2^{n(S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon - I(V;W) + \eta_n)},
\end{aligned}$$

for some sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ (see Lemma A.4 in Appendix A). If $S_1 - R_1 + S_2 - R_2 + S_C - R_C - \varepsilon < I(V;W)$, then the above probability vanishes as n tends to infinity.

D.1.2 Proof of (2.9)

The probability that Bob fails to decode index s_1 when he has already decoded index s writes:

$$\begin{aligned}
\Pr\{\not{s_1}, \check{s}\} &= \Pr\Big\{\exists\, s_1' \neq s_1, s_2' \text{ s.t. } (u^n(s_1'), v^n(s_1', s_2'), w^n(s)) \\
&\qquad\qquad \in (B_1(r_1) \times B_2(s_1', r_2) \times B_C(r)) \cap T_\delta^n(U,V,W)\Big\} \\
&\leq 2^{n(S_1 - R_1 + S_2 - R_2)} \\
&\qquad \times \Pr\Big\{(U^n, V^n, W^n) \in T_\delta^n(U,V,W) \,\Big|\, (U^n, V^n) \in T_\delta^n(U,V), W^n \in T_\delta^n(W)\Big\},
\end{aligned}$$

Following the above argument, if $S_1 - R_1 + S_2 - R_2 < I(V;W)$, then the above probability vanishes as n tends to infinity.

D.1.3 Proof of (2.10)

Finally, the probability that Bob fails to decode index s_2 when he has already decoded indices (s, s_1) writes:

$$\begin{aligned}
&\Pr\{\check{s}_1, \not{s_2}, \check{s}\} \\
&\quad = \Pr\Big\{\exists\, s_2' \neq s_2 \text{ s.t. } (u^n(s_1), v^n(s_1, s_2'), w^n(s)) \\
&\qquad\qquad \in (B_1(r_1) \times B_2(s_1, r_2) \times B_C(r)) \cap T_\delta^n(U, V, W)\Big\} \\
&\quad \leq 2^{n(S_2 - R_2)} \\
&\qquad \times \Pr\Big\{(U^n, V^n, W^n) \in T_\delta^n(U, V, W) \;\Big|\; (U^n, V^n) \in T_\delta^n(U, V), (U^n, W^n) \in T_\delta^n(U, W)\Big\} \\
&\quad \leq 2^{n(S_2 - R_2)}\, 2^{-n(I(V;W|U) - \eta_n)}\,,
\end{aligned}$$

for some sequence $\eta_n \xrightarrow[n\to\infty]{} 0$. If $S_2 - R_2 < I(V; W|U)$, then the above probability vanishes as n tends to infinity.

This concludes the proof of Lemma 2.4. □

D.2 Proof of Lemma 2.5

Since the codeword index s_1 is a deterministic function of A^n, term $H(A^n|s_1E^n)$ writes

$$\begin{aligned}
H(A^n|s_1E^n) &= H(A^nE^n|s_1) - H(E^n|s_1) \\
&= H(A^nE^n) - H(s_1) - H(E^n|s_1)\,. \qquad \text{(D.1)}
\end{aligned}$$

We now study each term of the r.h.s. of the above equation.

D.2.1 First term

Variables (A_i, E_i) are i.i.d., hence $H(A^nE^n) = nH(AE)$.

D.2.2 Second term

Quantity $H(s_1)$ is studied through the distribution of index s_1, using classical argument of typical sequences and random coding. From the encoding procedure described in Section 2.3.2.1, the distribution of s_1 writes, for each $j \in \{1, \ldots, 2^{nS_1}\}$:

$$\begin{aligned}
\Pr\{s_1 = j\} &= \Pr\left\{\Big((u^n(j), A^n) \in T_\delta^n(U, A)\Big) \cap \bigcap_{i=1}^{j-1} \Big((u^n(i), A^n) \notin T_\delta^n(U, A)\Big)\right\} \\
&= t_n(1 - t_n)^{j-1}\,,
\end{aligned}$$

where $t_n \triangleq \Pr\left\{(U^n, A^n) \in T_\delta^n(U,A) \;\middle|\; U^n \in T_\delta^n(U), A^n \in T_\delta^n(A)\right\}$. The entropy of index s_1 thus writes

$$H(s_1) = -\sum_{j=1}^{2^{nS_1}} t_n(1-t_n)^{j-1}\log(t_n(1-t_n)^{j-1}) - P_{e,1}\log(P_{e,1}) \;,$$

where $P_{e,1}$ is the error probability of this encoding step. From Section 2.3.4, if $S_1 > I(U;A)$, then probability $P_{e,1}$ vanishes as n tends to infinity. Since each term $t_n(1-t_n)^{j-1}$ is non-negative and $x\log x \xrightarrow[x\to 0^+]{} 0^-$, the above entropy can be upper bounded as follows:

$$H(s_1) \leq -\sum_{j=1}^{\infty} t_n(1-t_n)^{j-1}\log(t_n(1-t_n)^{j-1}) + \eta_n^{(1)} \;, \tag{D.2}$$

for some sequence $\eta_n^{(1)} \xrightarrow[n\to\infty]{} 0$. The above series writes

$$\sum_{j=1}^{\infty} t_n(1-t_n)^{j-1}\log(t_n(1-t_n)^{j-1})$$
$$= t_n\log(t_n)\sum_{j=1}^{\infty}(1-t_n)^{j-1} + t_n\log(1-t_n)\sum_{j=1}^{\infty}(j-1)(1-t_n)^{j-1} \;.$$

Equation (D.2) thus yields the following upper bound:

$$H(s_1) \leq -\log(t_n) - \log(1-t_n)\frac{1-t_n}{t_n} + \eta_n^{(1)} \;.$$

Now, from standard results on typical sequences (see Appendix A), $2^{-n(I(U;A)+\eta_n^{(2)})} \leq t_n \leq 2^{-n(I(U;A)-\eta_n^{(2)})}$ for some sequence $\eta_n^{(2)} \xrightarrow[n\to\infty]{} 0$. Since $\frac{\log(1-x)}{x} \xrightarrow[x\to 0]{} -1$, this yields

$$H(s_1) \leq n(I(U;A)+\eta_n^{(2)}) + 1 + \eta_n^{(3)} + \eta_n^{(1)} \;,$$

for some sequence $\eta_n^{(3)} \xrightarrow[n\to\infty]{} 0$.

D.2.3 Third term

The third term can be studied following the argument of [90, Section 2.3] for the wiretap channel. The equivalent of Equation (2.54) of [90] here writes

$$H(E^n|s_1) \leq n\left(H(E|U) + \eta_n^{(4)}\right) \;,$$

for some sequence $\eta_n^{(4)} \xrightarrow[n\to\infty]{} 0$.

Equation (D.1) along with the above results yields

$$\frac{1}{n}H(A^n|s_1E^n) \geq H(AE) - I(U;A) - \eta_n^{(2)} - \frac{1+\eta_n^{(3)}+\eta_n^{(1)}}{n} - H(E|U) - \eta_n^{(4)} \;. \tag{D.3}$$

Using the Markov chain $U \multimap A \multimap E$, this concludes the proof of Lemma 2.5. □

D.3 Proof of Proposition 2.2 (Bounds on the cardinalities)

D.3.1 Bound on $\|\mathcal{W}\|$

First, note that the single-letter inequalities of Theorem 2.1 can be written as follows:

$$\begin{aligned}
R_A &\geq I(V;A|W)\,,\\
R_C &\geq H(C|V) - H(C|VW)\,,\\
R_A + R_C &\geq I(V;A) + H(C|V) - H(C|VW)\,,\\
D &\geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\,,\\
\Delta &\leq H(A|UE) - I(V;A|W) + I(U;A|W)\,,\\
\Delta - R_C &\leq H(A|V) - I(A;E|U) - H(C|V) + H(C|VW)\,.
\end{aligned}$$

We then use Fenchel-Eggleston-Carathéodory's theorem and follow standard arguments [42, Appendix C]. Consider the following $\|\mathcal{C}\| + 3$ continuous functions of $p(c|w)$:

$$\begin{aligned}
&p(c|w)\,,\\
&I(V;A|W=w)\,,\\
&H(C|V,W=w) = H(CV|W=w) - H(V|W=w)\,,\\
&\mathbb{E}\big[d(A,\hat{A}(V,W))\big|W=w\big]\,,\\
&I(U;A|W=w)
\end{aligned}$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a random variable W' on $\mathcal{W}'$ with $\|\mathcal{W}'\| \leq \|\mathcal{C}\| + 3$ such that $p(c)$, $I(V;A|W)$, $H(C|VW)$, $\mathbb{E}\big[d(A,\hat{A}(V,W))\big]$ and $I(U;A|W)$ are preserved.

D.3.2 Bounds on $\|\mathcal{U}\|$ and $\|\mathcal{V}\|$

We now rewrite the inequalities of Theorem 2.1 as follows:

$$\begin{aligned}
R_A &\geq H(A|W) - H(A|VW)\,,\\
R_C &\geq I(W;C|V)\,,\\
R_A + R_C &\geq I(W;C) + H(A|W) - H(A|VW)\,,\\
D &\geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\,,\\
\Delta &\leq H(A|VW) + I(A;W|U) - I(A;E|U)\,,\\
\Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V)\,.
\end{aligned}$$

Consider the following $\|\mathcal{A}\| + 5$ continuous functions of $p(v|u)$:

$$
\begin{aligned}
&p(a|u) = \mathbb{E}\big[p(a|V)\big|U = u\big] \,, \\
&H(A|VW, U = u) = H(AVW|U = u) - H(VW|U = u) \,, \\
&I(W; C|V, U = u) = I(W; C|U = u) - I(W; V|U = u) \,, \\
&\mathbb{E}\big[d(A, \hat{A}(V, W))\big|U = u\big] \,, \\
&I(A; W|U = u) \,, \\
&I(A; E|U = u) \,, \\
&H(A|V, U = u) = H(AV|U = u) - H(V|u = u) \,.
\end{aligned}
$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a random variable U' on $\mathcal{U}'$ with $\|\mathcal{U}'\| \leq \|\mathcal{A}\| + 5$ such that $p(a)$, $H(A|VW)$, $I(W; C|V)$, $\mathbb{E}\big[d(A, \hat{A}(V, W))\big]$, $I(A; W|U)$, $I(A; E|U)$, and $H(A|V)$ are preserved.

Now, for each $u' \in \mathcal{U}'$, consider the following $\|\mathcal{A}\|+3$ continuous functions of $p(a|u', v)$:

$$
\begin{aligned}
&p(a|u', v) \,, \\
&H(A|W, U' = u', V = v) = H(AW|U' = u', V = v) - H(W|U' = u', V = v) \,, \\
&I(W; C|U' = u', V = v) \,, \\
&\mathbb{E}\big[d(A, \hat{A}(V, W))\big|U' = u', V = v\big] \,, \\
&H(A|U' = u', V = v) \,.
\end{aligned}
$$

From Fenchel-Eggleston-Carathéodory's theorem, there exists a set $\mathcal{V}'$ with $\|\mathcal{V}'\| \leq \|\mathcal{A}\| + 3$ and, for each $u' \in \mathcal{U}'$, a random variable $V'|\{U' = u'\}$ on $\mathcal{V}'$ and a function $\hat{A}'_{u'} \colon \mathcal{V}' \times \mathcal{W} \to \mathcal{A}$, such that $p(a|u')$, $H(A|VW, U' = u')$, $I(W; C|V, U' = u')$, $\mathbb{E}\big[d(A, \hat{A}(V, W))\big|U' = u'\big]$, and $H(A|V, U' = u')$ are preserved.

Then define set $\mathcal{V}'' = \mathcal{U}' \times \mathcal{V}'$, random variable $V'' = (U', V')$ and function $\hat{A}'' \colon \mathcal{V}'' \times \mathcal{W} \to \mathcal{A}$ by $\hat{A}''(v'', w) = \hat{A}''(u', v', w) \triangleq \hat{A}'_{u'}(v', w)$. From the above cardinality bounds, $\|\mathcal{V}''\| \leq (\|\mathcal{A}\| + 5)(\|\mathcal{A}\| + 3)$. Note that $U' \multimap V'' \multimap A \multimap (C, E)$ form a Markov chain. From these new definitions and previous constructions, we easily check that quantities involving variable V ($H(A|VW)$, $I(W; C|V)$, $\mathbb{E}[d(A, \hat{A}(V, W))]$, $H(A|V)$) are preserved. This concludes the proof of Proposition 2.2. □

D.4 Proof of Theorem 2.3 (Outer bound)

In this section, we prove Theorem 2.3. Let (R_A, R_C, D, Δ) be an achievable tuple and $\varepsilon > 0$. There exists an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) s.t.:

$$
\begin{aligned}
\mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] &\leq D + \varepsilon \,, \\
\frac{1}{n} H(A^n|f_A(A^n), E^n) &\geq \Delta - \varepsilon \,.
\end{aligned}
$$

Denote by $J = f_A(A^n)$ and $K = f_C(C^n)$ the messages transmitted by Alice and Charlie, respectively. From these definitions and the fact that random variables A_i, C_i, E_i are independent across time, the joint distribution of (J, K, A^n, C^n, E^n) can be written as follows:

$$p(j,k,a^n,c^n,e^n) = \mathbf{1}_{\{f_A(a^n)\}}(j)\,\mathbf{1}_{\{f_C(c^n)\}}(k)\,p(a^{i-1},c^{i-1},e^{i-1})\,p(a_i,c_i,e_i)\,p(a_{i+1}^n,c_{i+1}^n,e_{i+1}^n)\,.$$

Following the technique described in Appendix B and using the above expansion, we can obtain the graphs of Figures D.1 and D.2.

For each $i \in \{1,\ldots,n\}$, define random variables U_i, V_i and W_i as follows:

$$U_i = (J, A^{i-1}, \quad E^{i-1})\,, \tag{D.4}$$

$$V_i = (J, A^{i-1}, C^{i-1}, E^{i-1})\,, \tag{D.5}$$

$$W_i = (K, \quad C^{i-1} \quad)\,. \tag{D.6}$$

From Figure D.1, $U_i \multimap V_i \multimap A_i \multimap (C_i, E_i)$ and $W_i \multimap C_i \multimap (A_i, E_i)$ form Markov chains (see Appendix B for details on this graphical technique for checking Markov relations).

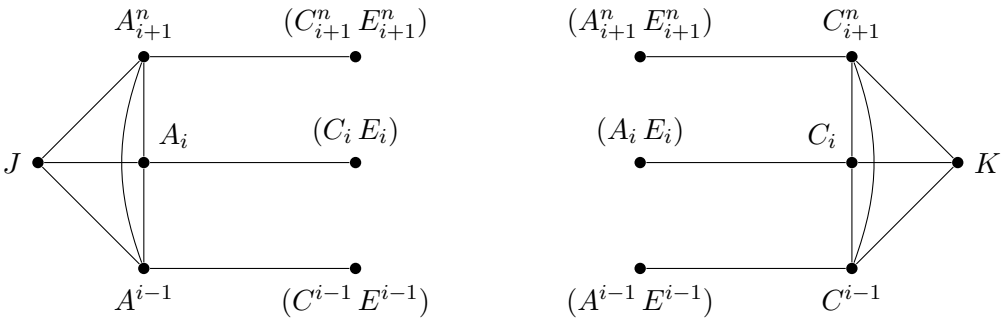
Following the usual technique, we also define an independent random variable Q uniformly distributed over the set $\{1,\ldots,n\}$, and $A = A_Q$, $C = C_Q$, $E = E_Q$, $U = (Q, U_Q)$, $V = (Q, V_Q)$, and $W = (Q, W_Q)$. Note that $U \multimap V \multimap A \multimap (C, E)$ and $W \multimap C \multimap (A, E)$ still form Markov chains, and that (A, C, E) is distributed according to the joint distribution $p(a, c, e)$ i.e., the original distribution of (A_i, C_i, E_i).

D.4.1 Rate at Alice

We first derive a lower bound for the rate at Alice:

$$\begin{aligned}
n(R_A+\varepsilon) &\geq H(J) \\
&\overset{(a)}{=} I(J; KA^nC^nE^n) \\
&\overset{(b)}{\geq} I(J; A^nC^nE^n|K) \\
&\overset{(c)}{=} \sum_{i=1}^{n} I(J; A_iC_iE_i|KA^{i-1}C^{i-1}E^{i-1}) \\
&= \sum_{i=1}^{n} \Big[I(JA^{i-1}E^{i-1}; A_iC_iE_i|KC^{i-1}) - I(A^{i-1}E^{i-1}; A_iC_iE_i|KC^{i-1})\Big] \\
&\overset{(d)}{=} \sum_{i=1}^{n} I(JA^{i-1}C^{i-1}E^{i-1}; A_iC_iE_i|KC^{i-1}) \\
&\overset{(e)}{\geq} \sum_{i=1}^{n} I(V_i; A_i|W_i)\,,
\end{aligned}$$

where



(a) $p(j, a^n, c^n, e^n)$ (b) $p(k, a^n, c^n, e^n)$

Figure D.1: Outer bound–Graphical representation of some probability distributions.

- step (a) follows from $J = f_A(A^n)$,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the Markov chain $(A_i, C_i, E_i) \multimap (K, C^{i-1}) \multimap (A^{i-1}, E^{i-1})$ (see Figure D.1b),
- step (e) from the non-negativity of mutual information and definitions (D.5), (D.6).

Using random variable Q, this yields

$$\begin{aligned} R_A + \varepsilon &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_Q; A_Q | W_Q, Q = i) \\ &= I(V_Q; A_Q | W_Q Q) \\ &= I(V; A|W)\ . \end{aligned}$$

D.4.2 Rate at Charlie

Using similar arguments with $K = f_C(C^n)$, we can obtain:

$$\begin{aligned} n(R_C + \varepsilon) &\geq H(K) \\ &\overset{(a)}{=} I(K; JA^nC^nE^n) \\ &\overset{(b)}{\geq} I(K; A^nC^nE^n|J) \\ &\overset{(c)}{=} \sum_{i=1}^{n} I(K; A_iC_iE_i|JA^{i-1}C^{i-1}E^{i-1}) \\ &\overset{(d)}{\geq} \sum_{i=1}^{n} I(W_i; C_i|V_i)\ , \end{aligned}$$

where

- step (a) follows from $K = f_C(C^n)$,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the non-negativity of mutual information and definitions (D.5), (D.6).

Then, using auxiliary random variable Q,

$$\begin{aligned} R_C + \varepsilon &\geq \frac{1}{n} \sum_{i=1}^{n} I(W_Q; C_Q | V_Q, Q = i) \\ &= I(W; C|V) \ . \end{aligned}$$

D.4.3 Sum-rate

The sum of the two rates R_A and R_C can also be lower bounded:

$$\begin{aligned} n(R_A + R_C + 2\varepsilon) &\geq H(JK) \\ &\overset{(a)}{=} I(JK; A^n C^n E^n) \\ &\overset{(b)}{=} \sum_{i=1}^{n} I(JK; A_i C_i E_i | A^{i-1} C^{i-1} E^{i-1}) \\ &= \sum_{i=1}^{n} \Big[I(JK A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) - I(A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) \Big] \\ &\overset{(c)}{=} \sum_{i=1}^{n} I(JK A^{i-1} C^{i-1} E^{i-1}; A_i C_i E_i) \\ &\overset{(d)}{\geq} \sum_{i=1}^{n} I(V_i W_i; A_i C_i) \ , \end{aligned}$$

where

- step (a) follows from $J = f_A(A^n)$ and $K = f_C(C^n)$,
- step (b) from the chain rule for mutual information,
- step (c) from the fact that random variables (A_i, C_i, E_i) are independent across time,
- step (d) from the non-negativity of mutual information and definitions (D.5), (D.6).

Using random variable Q, this yields

$$\begin{aligned} R_A + R_C + 2\varepsilon &\geq \frac{1}{n} \sum_{i=1}^{n} I(V_Q W_Q; A_Q C_Q | Q = i) \\ &= I(VW; AC) \ . \end{aligned}$$

D.4.4 Distortion at Bob

Bob reconstructs $g(J,K)$. For each $i \in \{1,\dots,n\}$, define function $\hat{A}_i$ as the i-th coordinate of this estimate:

$$\hat{A}_i(V_i, W_i) \triangleq g_i(J,K) \ .$$

The component-wise mean distortion at Bob thus verifies

$$\begin{aligned} D + \varepsilon &\geq \mathbb{E}\big[d(A^n, g(J,K))\big] \\ &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i,W_i))\right] \\ &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_Q, \hat{A}_Q(V_Q,W_Q)) \,\middle|\, Q=i\right] \\ &= \mathbb{E}\left[d(A_Q, \hat{A}_Q(V_Q,W_Q))\right] \\ &= \mathbb{E}\left[d(A, \hat{A}(V,W))\right] \ , \end{aligned}$$

where we defined function $\hat{A}$ by

$$\hat{A}(V,W) = \hat{A}(Q,V_Q,W_Q) \triangleq \hat{A}_Q(V_Q,W_Q) \ .$$

D.4.5 Equivocation rate at Eve

The equivocation at Eve writes

$$\begin{aligned} n(\Delta - \varepsilon) &\leq H(A^n|JE^n) \\ &= H(A^n|J) - I(A^n;E^n|J) \\ &\overset{(a)}{=} H(A^n|J) - I(A^n;E^n) + I(J;E^n) \\ &\overset{(b)}{\leq} \sum_{i=1}^{n}\Big[H(A_i|JA^{i-1}) - I(A_i;E_i) + I(JE^{i-1};E_i)\Big] \\ &= \sum_{i=1}^{n}\Big[H(A_i|JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i;KC^{i-1}E^{i-1}|JA^{i-1}) \\ &\qquad\qquad - I(A_i;E_i) + I(JE^{i-1};E_i)\Big] \ , \end{aligned}$$

where

- step (a) follows from the Markov chain $J \multimap A^n \multimap E^n$ (see Figure D.1a),
- step (b) from the chain rules for conditional entropy and mutual information, and the fact that random variables (A_i, E_i) are independent across time.

The above equation yields:

$$\begin{aligned} n(\Delta-\varepsilon) &\overset{(c)}{\leq} \sum_{i=1}^{n}\Big[H(A_i|JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i;KC^{i-1}|JA^{i-1}E^{i-1}) \\ &\qquad + I(A_i;E^{i-1}|JA^{i-1}) - I(A_i;E_i) + I(JA^{i-1}E^{i-1};E_i)\Big] \\ &\overset{(d)}{=} \sum_{i=1}^{n}\Big[H(A_i|JKA^{i-1}C^{i-1}E^{i-1}) + I(A_i;KC^{i-1}|JA^{i-1}E^{i-1}) \\ &\qquad - I(A_i;E_i|JA^{i-1}E^{i-1})\Big] \\ &\overset{(e)}{=} \sum_{i=1}^{n}\Big[H(A_i|V_iW_i) + I(A_i;W_i|U_i) - I(A_i;E_i|U_i)\Big]\,, \end{aligned}$$

where

- step (c) follows from standard identities and the non-negativity of conditional mutual information,
- step (d) from the Markov chain $E_i \multimap A_i \multimap (J, A^{i-1}) \multimap E^{i-1}$ (see Figure D.1a),
- step (e) from definitions (D.4), (D.5) and (D.6).

Now, using auxiliary random variable Q,

$$\begin{aligned} \Delta-\varepsilon &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[H(A_Q|V_QW_Q,Q=i) \\ &\qquad + I(A_Q;W_Q|U_Q,Q=i) - I(A_Q;E_Q|U_Q,Q=i)\Big] \\ &= H(A|VW) + I(A;W|U) - I(A;E|U)\,. \end{aligned}$$

D.4.6 Public-link secrecy rate

Quantity $\Delta - R_C$ can be upper bounded as follows:

$$\begin{aligned} n(\Delta - R_C - 2\varepsilon) &\leq H(A^n|JE^n) - H(K) \\ &\overset{(a)}{\leq} H(A^n|JE^n) - H(K|J) \\ &\overset{(b)}{=} H(A^n|JE^n) - I(K;A^nC^n|J)\,, \end{aligned}$$

where

- step (a) follows from the fact that conditioning reduces the entropy,
- step (b) from $K = f_C(C^n)$.

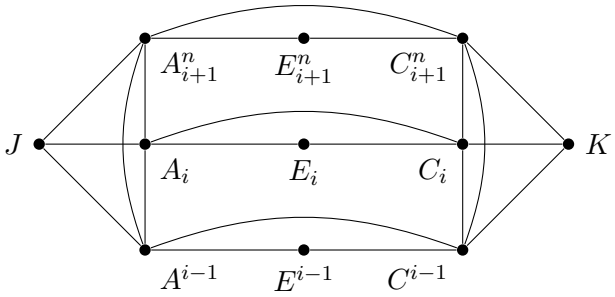


Figure D.2: Outer bound–Graphical representation of distribution $p(j, k, a^n, c^n, e^n)$.

The r.h.s. of the above equation can be expanded as follows:

$$\begin{aligned} n(\Delta - R_C - 2\varepsilon) &\overset{(c)}{\leq} \sum_{i=1}^{n} \Big[H(A_i|JA^{i-1}E^n) - I(K; A_iC_i|JA^{i-1}C^{i-1}) \Big] \\ &\overset{(d)}{\leq} \sum_{i=1}^{n} \Big[H(A_i|JA^{i-1}E^i) - I(K; C_i|JA^{i-1}C^{i-1}) \Big] \\ &\overset{(e)}{=} \sum_{i=1}^{n} \Big[H(A_i|JA^{i-1}C^{i-1}E^{i-1}) - I(A_i; E_i|JA^{i-1}E^{i-1}) \\ &\qquad\qquad - I(KC^{i-1}; C_i|JA^{i-1}C^{i-1}E^{i-1}) \Big] \\ &\overset{(f)}{=} \sum_{i=1}^{n} \Big[H(A_i|V_i) - I(A_i; E_i|U_i) - I(W_i; C_i|V_i) \Big] , \end{aligned}$$

where

- step (c) follows from the chain rules for conditional entropy and conditional mutual information,
- step (d) from the non-negativity of conditional mutual information,
- step (e) from the Markov chains $A_i \multimap (J, A^{i-1}) \multimap (C^{i-1}, E^{i-1})$ (see Figure D.1a) and $(K, C_i) \multimap (J, A^{i-1}, C^{i-1}) \multimap E^{i-1}$ (see Figure D.2),
- step (f) from definitions (D.4), (D.5) and (D.6).

Using auxiliary random variable Q,

$$\begin{aligned} \Delta - R_C - 2\varepsilon &\leq \frac{1}{n} \sum_{i=1}^{n} \Big[H(A_Q|V_Q, Q = i) - I(A_Q; E_Q|U_Q, Q = i) - I(W_Q; C_Q|V_Q, Q = i) \Big] \\ &= H(A|V) - I(A; E|U) - I(W; C|V) . \end{aligned}$$

D.4.7 End of proof

In the above paragraphs, we proved that, for each achievable tuple (R_A, R_C, D, Δ) and each $\varepsilon > 0$, there exist random variables U, V and W such that $U \multimap V \multimap A \multimap (C, E)$ and $W \multimap C \multimap (A, E)$ form Markov chains, and a function $\hat{A}$ such that

$$\begin{aligned} R_A + \varepsilon &\geq I(V; A|W) \,, \\ R_C + \varepsilon &\geq I(W; C|V) \,, \\ R_A + R_C + 2\varepsilon &\geq I(VW; AC) \,, \\ D + \varepsilon &\geq \mathbb{E}\big[d(A, \hat{A}(V, W))\big] \,, \\ \Delta - \varepsilon &\leq H(A|VW) + I(A; W|U) - I(A; E|U) \,, \\ \Delta - R_C - 2\varepsilon &\leq H(A|V) - I(A; E|U) - I(W; C|V) \,, \end{aligned}$$

i.e., $(R_A + \varepsilon, R_C + \varepsilon, D + \varepsilon, \Delta - \varepsilon) \in \mathcal{R}_{\text{out}}$. Recalling that region $\mathcal{R}_{\text{out}}$ is closed, and letting ε tend to zero prove Theorem 2.3. □

D.5 Proof of the converse part of Theorem 2.6

Let (R_A, D, Δ) be an achievable tuple and $\varepsilon > 0$. There exists an $(n, R_A + \varepsilon)$-code (f, g) such that

$$\begin{aligned} \mathbb{E}\left[d(A^n, g(f(A^n), C^n))\right] &\leq D + \varepsilon \,, \\ \frac{1}{n} H(A^n | f(A^n), E^n) &\geq \Delta - \varepsilon \,. \end{aligned}$$

Denote by $J = f(A^n)$ the transmitted message, and define variables U_i and V_i as follows, for each $i \in \{1, \ldots, n\}$:

$$U_i = (J, \quad C_{i+1}^n, E^{i-1}) \,, \tag{D.7}$$

$$V_i = (J, A^{i-1}, C^{i-1}, C_{i+1}^n, E^{i-1}) \,. \tag{D.8}$$

From Figure D.1a, $U_i \multimap V_i \multimap A_i \multimap (C_i, E_i)$ form a Markov chain.

We also define an independent random variable Q uniformly distributed over the set $\{1, \ldots, n\}$, and $A = A_Q$, $C = C_Q$, $E = E_Q$, $U = (Q, U_Q)$, and $V = (Q, V_Q)$. $U \multimap V \multimap A \multimap (C, E)$ still form a Markov chain and (A, C, E) is distributed according to the joint distribution $p(a, c, e)$ i.e., the original distribution of (A_i, C_i, E_i).

D.5.1 Rate

We prove a lower bound on the rate:

$$\begin{aligned}
n(R_A+\varepsilon) &\geq H(J) \\
&\overset{(a)}{=} I(J;A^nC^nE^n) \\
&\overset{(b)}{\geq} I(J;A^nE^n|C^n) \\
&\overset{(c)}{=} \sum_{i=1}^{n} I(J;A_iE_i|A^{i-1}C^nE^{i-1}) \\
&= \sum_{i=1}^{n} \Big[I(JA^{i-1}C^{i-1}C_{i+1}^nE^{i-1};A_iE_i|C_i) - I(A^{i-1}C^{i-1}C_{i+1}^nE^{i-1};A_iE_i|C_i) \Big] \\
&\overset{(d)}{=} \sum_{i=1}^{n} I(JA^{i-1}C^{i-1}C_{i+1}^nE^{i-1};A_iE_i|C_i) \\
&\overset{(e)}{\geq} \sum_{i=1}^{n} I(V_i;A_i|C_i) \,,
\end{aligned}$$

where

- step (a) follows from $J = f(A^n)$,
- step (b) from the non-negativity of mutual information,
- step (c) from the chain rule for conditional mutual information,
- step (d) from the fact that random variables (A_i, C_i, E_i) are independent across time,
- step (e) from the non-negativity of mutual information and definition (D.8).

Then, using random variable Q,

$$\begin{aligned}
R_A+\varepsilon &\geq \frac{1}{n}\sum_{i=1}^{n} I(V_Q;A_Q|C_Q,Q=i) \\
&= I(V_Q;A_Q|C_QQ) \\
&= I(V;A|C) \,.
\end{aligned}$$

D.5.2 Distortion at Bob

Bob reconstructs $g(J, C^n)$. For each $i \in \{1, \ldots, n\}$, define function $\hat{A}_i$ as the i-th coordinate of this estimate:

$$\hat{A}_i(V_i, C_i) \triangleq g_i(J, C^{i-1}, C_i, C_{i+1}^n) \,.$$

The component-wise mean distortion at Bob thus verifies

$$\begin{aligned} D+\varepsilon &\geq \mathbb{E}\left[d(A^n, g(J, C^n))\right] \\ &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i, C_i))\right] \\ &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_Q, \hat{A}_Q(V_Q, C_Q)) \,\middle|\, Q=i\right] \\ &= \mathbb{E}\left[d(A_Q, \hat{A}_Q(V_Q, C_Q))\right] \\ &= \mathbb{E}\left[d(A, \hat{A}(V, C))\right] \ , \end{aligned}$$

where we defined function $\hat{A}$ on $\mathcal{V}\times\mathcal{C}$ by

$$\hat{A}(V,C) = \hat{A}(Q, V_Q, C_Q) \triangleq \hat{A}_Q(V_Q, C_Q) \ .$$

D.5.3 Equivocation rate at Eve

The equivocation at Eve can be upper bounded as follows:

$$\begin{aligned} n(\Delta-\varepsilon) &\leq H(A^n|JE^n) \\ &= H(A^n|J) - I(A^n;E^n|J) \\ &= H(A^n|JC^n) + I(A^n;C^n|J) - I(A^n;E^n|J) \\ &\overset{(a)}{=} H(A^n|JC^n) + I(A^n;C^n) - I(J;C^n) - I(A^n;E^n) + I(J;E^n) \\ &\overset{(b)}{=} \sum_{i=1}^{n}\Big[H(A_i|JA^{i-1}C^n) + I(A_i;C_i) - I(JC_{i+1}^n;C_i) - I(A_i;E_i) + I(JE^{i-1};E_i)\Big] \\ &\overset{(c)}{=} \sum_{i=1}^{n}\Big[H(A_i|JA^{i-1}C^nE^{i-1}) + I(A_i;C_i) - I(JC_{i+1}^n;C_i) - I(A_i;E_i) \\ &\qquad + I(JE^{i-1};E_i) + I(E_i;C_{i+1}^n|JE^{i-1}) - I(C_i;E^{i-1}|JC_{i+1}^n)\Big] \\ &= \sum_{i=1}^{n}\Big[H(A_i|JA^{i-1}C^nE^{i-1}) + I(A_i;C_i) - I(A_i;E_i) \\ &\qquad + I(E_i;JC_{i+1}^nE^{i-1}) - I(C_i;JC_{i+1}^nE^{i-1})\Big] \\ &\overset{(d)}{=} \sum_{i=1}^{n}\Big[H(A_i|V_iC_i) + I(A_i;C_i) - I(A_i;E_i) + I(E_i;U_i) - I(C_i;U_i)\Big] \\ &\overset{(e)}{=} \sum_{i=1}^{n}\Big[H(A_i|V_iC_i) + I(A_i;C_i|U_i) - I(A_i;E_i|U_i)\Big] \ , \end{aligned}$$

where

- step (a) follows from the Markov chain $J \multimap A^n \multimap (C^n, E^n)$,
- step (b) from the chain rules for conditional entropy and mutual information, and the fact that random variables (A_i, C_i, E_i) are independent across time,
- step (c) from the Markov chain $(A_i, C^i) \multimap (J, A^{i-1}) \multimap (C^{i-1}, E^{i-1})$ (see Figure D.1a) and Csiszár and Körner's equality (see Appendix C.1),
- step (d) from definitions (D.7) and (D.8),
- step (e) from the Markov chain $U_i \multimap A_i \multimap (C_i, E_i)$.

Using auxiliary random variable Q, this yields

$$\begin{aligned}\Delta - \varepsilon &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[H(A_Q|V_QC_Q, Q=i) \\ &\quad + I(A_Q; C_Q|U_Q, Q=i) - I(A_Q; E_Q|U_Q, Q=i)\Big] \\ &= H(A|VC) + I(A;C|U) - I(A;E|U)\,.\end{aligned}$$

D.5.4 End of proof

We proved that, for each achievable tuple (R_A, D, Δ) and each $\varepsilon > 0$, there exist random variables U, V such that $U \multimap V \multimap A \multimap (C, E)$ forms a Markov chain, and

$$\begin{aligned}R_A + \varepsilon &\geq I(V;A|C)\,,\\ D + \varepsilon &\geq \mathbb{E}\big[d(A, \hat{A}(V,C))\big]\,,\\ \Delta - \varepsilon &\leq H(A|VC) + I(A;C|U) - I(A;E|U)\,.\end{aligned}$$

Recalling that region $\mathcal{R}^*_{\text{uncoded}}$ is closed, and letting ε tend to zero prove the converse part of Theorem 2.6. □

D.6 Proof of the converse part of Theorem 2.12

Let (R_A, R_C, Δ) be an achievable tuple and $\varepsilon > 0$. There exists an $(n, R_A+\varepsilon, R_C+\varepsilon)$-code (f_A, f_C, g) such that:

$$\Pr\{g(f_A(A^n), f_C(C^n)) \neq (A^n, C^n)\} \leq \varepsilon\,, \tag{D.9}$$

$$\frac{1}{n}H(A^n|f_A(A^n), E^n) \geq \Delta - \varepsilon\,. \tag{D.10}$$

Denote by $J = f_A(A^n)$ and $K = f_C(C^n)$ the messages transmitted by Alice and Charlie, respectively. For each $i \in \{1, \ldots, n\}$, define random variable U_i by

$$U_i = (J, C_{i+1}^n, E^{i-1})\,. \tag{D.11}$$

From Figure D.1a, $U_i \multimap A_i \multimap (C_i, E_i)$ form a Markov chain.

We also define an independent random variable Q uniformly distributed over the set $\{1, \ldots, n\}$, and $A = A_Q$, $C = C_Q$, $E = E_Q$, $U = (Q, U_Q)$. Note that $U \multimap A \multimap (C, E)$ still form a Markov chain, and that (A, C, E) is distributed according to the joint distribution $p(a, c, e)$ i.e., the original distribution of (A_i, C_i, E_i).

D.6.1 Rate at Alice

Following the argument of the converse for the Slepian-Wolf theorem [31, Section 15.4.2], we prove lower bounds on the rates:

$$\begin{aligned} n(R_A + \varepsilon) &\geq H(J) \\ &\overset{(a)}{\geq} H(J|C^n) \\ &\overset{(b)}{=} I(A^n; J|C^n) \\ &\overset{(c)}{=} H(A^n|C^n) - H(A^n|JKC^n) \\ &\overset{(d)}{\geq} nH(A|C) - nO(\varepsilon) \,, \end{aligned}$$

where

- step (a) follows from the fact that conditioning reduces the entropy,
- step (b) from $J = f_A(A^n)$,
- step (c) from $K = f_C(C^n)$,
- step (d) from the fact that random variables (A_i, C_i) are i.i.d., and Fano's inequality together with (D.9).[1]

D.6.2 Rate at Charlie

Using similar arguments with $K = f_C(C^n)$, we can obtain:

$$\begin{aligned} n(R_C + \varepsilon) &\geq H(K) \\ &\overset{(a)}{\geq} H(K|J) \\ &\overset{(b)}{=} I(K; C^n|J) \\ &= H(C^n|J) - H(C^n|JK) \\ &\overset{(c)}{\geq} \sum_{i=1}^{n} H(C_i|JC_{i+1}^n) - nO(\varepsilon) \\ &\overset{(d)}{\geq} \sum_{i=1}^{n} H(C_i|U_i) - nO(\varepsilon) \,, \end{aligned}$$

where

[1] Landau-like notation $O(\varepsilon)$ stands for a term X such that $0 \leq X \leq k\varepsilon$ for some constant $k > 0$.

- step (a) follows from the fact that conditioning reduces the entropy,
- step (b) from $K = f_C(C^n)$,
- step (c) from the chain rule for conditional entropy and Fano's inequality,
- step (d) from the fact that conditioning reduces the entropy, and definition (D.11).

Now, using auxiliary random variable Q,

$$\begin{aligned} R_C + \varepsilon &\geq \frac{1}{n}\sum_{i=1}^{n} H(C_Q|U_Q, Q=i) - O(\varepsilon) \\ &= H(C|U) - O(\varepsilon)\ . \end{aligned} \tag{D.12}$$

D.6.3 Sum-rate

A lower bound on the sum-rate can be derived as well:

$$\begin{aligned} n(R_A + R_C + 2\varepsilon) &\geq H(JK) \\ &\overset{(a)}{=} I(A^nC^n; JK) \\ &\overset{(b)}{\geq} nH(AC) - nO(\varepsilon)\ , \end{aligned}$$

where

- step (a) follows from $J = f_A(A^n)$ and $K = f_C(C^n)$,
- step (b) from the fact that random variables (A_i, C_i) are i.i.d., and Fano's inequality.

D.6.4 Equivocation rate at Eve

We then prove an upper bound for the equivocation et Eve:

$$\begin{aligned} n(\Delta - \varepsilon) &\leq H(A^n|JE^n) \\ &= H(A^n|J) - I(A^n; E^n|J) \\ &= H(A^n|JK) + I(A^n; K|J) - I(A^n; E^n|J) \\ &\overset{(a)}{\leq} nO(\varepsilon) + I(A^n; C^n|J) - I(A^n; E^n|J) \\ &\overset{(b)}{=} nO(\varepsilon) + I(A^n; C^n) - I(J; C^n) - I(A^n; E^n) + I(J; E^n)\ , \end{aligned}$$

where

- step (a) follows from Fano's inequality, and $K = f_C(C^n)$,
- step (b) from the Markov chain $J \multimap A^n \multimap (C^n, E^n)$.

The r.h.s. of the above equation can be expanded as follows:

$$\begin{aligned}
n(\Delta-\varepsilon) &\overset{(c)}{\leq} nO(\varepsilon)+\sum_{i=1}^{n}\Big[I(A_i;C_i)-I(JC_{i+1}^n;C_i)-I(A_i;E_i)+I(JE^{i-1};E_i)\Big]\\
&\overset{(d)}{=} nO(\varepsilon)+\sum_{i=1}^{n}\Big[I(A_i;C_i)-I(JC_{i+1}^n;C_i)-I(A_i;E_i)+I(JE^{i-1};E_i)\\
&\qquad\qquad +I(E_i;C_{i+1}^n|JE^{i-1})-I(C_i;E^{i-1}|JC_{i+1}^n)\Big]\\
&= nO(\varepsilon)+\sum_{i=1}^{n}\Big[I(A_i;C_i)-I(JC_{i+1}^nE^{i-1};C_i)-I(A_i;E_i)+I(JC_{i+1}^nE^{i-1};E_i)\Big]\\
&\overset{(e)}{=} nO(\varepsilon)+\sum_{i=1}^{n}\Big[I(A_i;C_i|U_i)-I(A_i;E_i|U_i)\Big]\,,
\end{aligned}$$

where

- step (c) follows from the chain rule for mutual information, and the fact that random variables (A_i, C_i, E_i) are independent across time,
- step (d) from Csiszár and Körner's equality (see Appendix C.1),
- step (e) from definition (D.11), and the Markov chain $U_i \multimap A_i \multimap (C_i, E_i)$.

Now, using auxiliary random variable Q,

$$\begin{aligned}
\Delta-\varepsilon &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[I(A_Q;C_Q|U_Q,Q=i)-I(A_Q;E_Q|U_Q,Q=i)\Big]+O(\varepsilon)\\
&= I(A;C|U)-I(A;E|U)+O(\varepsilon)\,.
\end{aligned}$$

D.6.5 End of proof

We proved that, for each achievable tuple (R_A, R_C, Δ) and each $\varepsilon > 0$, there exists a random variable U such that $U \multimap A \multimap (C, E)$ form a Markov chain, and

$$\begin{aligned}
R_A+O(\varepsilon) &\geq H(A|C)\,,\\
R_C+O(\varepsilon) &\geq H(C|U)\,,\\
R_A+R_C+O(\varepsilon) &\geq H(AC)\,,\\
\Delta-O(\varepsilon) &\leq I(A;C|U)-I(A;E|U)\,.
\end{aligned}$$

Recalling that region $\mathcal{R}^*_{\text{lossless}}$ is closed, and letting ε tend to zero prove the converse part of Theorem 2.12. □

D.7 Proof of the converse part of Proposition 2.13

The proof of the converse part of Proposition 2.13 follows the same argument that Appendix D.6. In particular, definition (D.11) remains the same. The only difference lies in the lower bound for the rate at Alice:

$$\begin{aligned}
n(R_A+\varepsilon) &\geq H(J) \\
&\overset{(a)}{=} I(J;A^n|C^n) + I(J;C^n) \\
&\overset{(b)}{=} H(A^n|C^n) - H(A^n|JKC^n) + I(J;C^n) \\
&\overset{(c)}{\geq} -nO(\varepsilon) + \sum_{i=1}^{n} \Big[H(A_i|C_i) + I(JC_{i+1}^n;C_i) \Big] \\
&\overset{(d)}{=} -nO(\varepsilon) + \sum_{i=1}^{n} \Big[H(A_i|C_i) + I(JC_{i+1}^n;C_i) \\
&\qquad\qquad + I(E^{i-1};C_i|JC_{i+1}^n) - I(C_{i+1}^n;E_i|JE^{i-1}) \Big] \\
&\overset{(e)}{\geq} -nO(\varepsilon) + \Big[\sum_{i=1}^{n} H(A_i|C_i) + I(JC_{i+1}^n E^{i-1};C_i) - I(JC_{i+1}^n E^{i-1};E_i) \Big] \\
&\overset{(f)}{=} -nO(\varepsilon) + \sum_{i=1}^{n} \Big[H(A_i|C_i) + I(U_i;C_i) - I(U_i;E_i) \Big] ,
\end{aligned}$$

where

- step (a) follows from $J = f_A(A^n)$,
- step (b) from $K = f_C(C^n)$,
- step (c) from Fano's inequality, the chain rule for conditional mutual information and the fact that random variables (A_i, C_i) are independent across time,
- step (d) from Csiszár and Körner's equality (see Appendix C.1),
- step (e) from the fact that random variables (A_i, C_i, E_i) are independent across time, and the non-negativity of mutual information,
- step (f) from definition (D.11).

Using random variable Q and following the argument of Appendix D.6, we proved the following lower bound:

$$R_A + \varepsilon \geq H(A|C) + I(U;C) - I(U;E) - O(\varepsilon) .$$

Since (D.12) still holds, we proved the bound on R_A given by Proposition 2.13. Other steps of the proof remain unchanged. □

D.8 Proof of Proposition 2.14

Corner point (I) defines a region $\mathcal{R}_{(I)}$ given by the following inequalities (see Table 2.1 in Section 2.2.2):

$$R_A \geq I(V;A|W)\ , \tag{D.13}$$

$$R_C \geq I(W;C)\ , \tag{D.14}$$

$$D \geq \mathbb{E}\big[d(A,\hat{A}(V,W))\big]\ , \tag{D.15}$$

$$\Delta \leq h(A|VW) + I(A;W|U) - I(A;E|U)\ . \tag{D.16}$$

For some fixed $R_C \geq 0$ and $D > 0$, auxiliary random variables U, V and W are chosen so that bounds on R_A and Δ given by Proposition 2.14 yields a point (R_A, R_C, D, Δ) in region $\mathcal{R}_{(I)}$. More precisely, function $\hat{A}$ is chosen as the minimum mean square error (MMSE) estimator of A given V and W, and auxiliary variables V and W are defined as the outputs of independent AWGN channels with respective inputs A and C. The gains of these two channels are tuned to meet constraints (D.14) and (D.15), respectively. Then, since variables A, E and W are Gaussian, either $W \succeq_A E$, or $E \succeq_A W$. The upper bound (D.16) is thus maximized setting $U = \emptyset$, or $U = V$.

D.8.1 Variable W–Rate at Charlie

We first define $\rho_W \in [0,1)$ by $\rho_W^2 = 1 - 2^{-2R_C}$, and choose random variable W as follows:

$$W = \rho_W C + N_W\ ,$$

where $N_W \sim \mathcal{N}(0, 1-\rho_W^2)$ is an independent random noise. With these definitions,

$$\begin{aligned} I(W;C) &= \frac{1}{2}\log\left(\frac{1}{\mathrm{Var}\,[C|W]}\right) \\ &= \frac{1}{2}\log\left(\frac{1}{1-\rho_W^2}\right) \\ &= R_C\ . \end{aligned}$$

D.8.2 Variable V–Distortion at Bob and rate at Alice

We then define $\rho_V \in [0,1)$ by

$$\rho_V^2 = \begin{cases} \frac{1-(\rho_W\rho_C)^2-D}{1-(\rho_W\rho_C)^2-D(\rho_W\rho_C)^2} & \text{if } D < 1-(\rho_W\rho_C)^2 \\ 0 & \text{otherwise} \end{cases} \tag{D.17}$$

and choose random variable V as follows:

$$W = \rho_V A + N_V\ ,$$

where $N_V \sim \mathcal{N}(0, 1-\rho_V^2)$ is an independent random noise. Note that if large distortion levels are allowed, then Alice will not transmit anything ($V = \emptyset$).

With these definitions,

$$\begin{aligned}\mathbb{E}\big[d(A, \hat{A}(V,W))\big] &= \mathrm{Var}\,[A|VW] \\ &= \frac{(1-\rho_V^2)(1-(\rho_W\rho_C)^2)}{1-(\rho_V\rho_W\rho_C)^2} \\ &\leq D\,,\end{aligned}$$

and

$$\begin{aligned}I(V;A|W) &= \frac{1}{2}\log\left(\frac{\mathrm{Var}\,[A|W]}{\mathrm{Var}\,[A|VW]}\right) \\ &= \frac{1}{2}\log\left(\frac{1-(\rho_W\rho_C)^2}{\mathrm{Var}\,[A|VW]}\right) \\ &= \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ .\end{aligned}$$

D.8.3 Variable U–Equivocation rate at Eve

The above rates and distortion level can be achieved with the following equivocation rate, depending on the choice of U:

- If $U = \emptyset$:

$$\begin{aligned}&h(A|VW) + I(A;W|U) - I(A;E|U) \\ &\qquad = h(A|E) - I(V;A|W) \\ &\qquad = \frac{1}{2}\log\big(2\pi e(1-\rho_E^2)\big) - \frac{1}{2}\left[\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}{D}\right)\right]_+ .\end{aligned}$$

- If $U = V$:

$$\begin{aligned}&h(A|VW) + I(A;W|U) - I(A;E|U) \\ &\quad = h(A|E) - I(V;A|E) \\ &\quad = \frac{1}{2}\log\big(2\pi e(1-\rho_E^2)\big) - \frac{1}{2}\log\left(\frac{1-(\rho_V\rho_E)^2}{1-\rho_V^2}\right) \\ &\quad = \frac{1}{2}\log\big(2\pi e(1-\rho_E^2)\big) - \frac{1}{2}\log\left(1+(1-\rho_E^2)\left[\frac{1}{D} - \frac{1}{1-\rho_C^2+\rho_C^2\,2^{-2R_C}}\right]_+\right),\end{aligned}$$

  where the last equality follows from definition (D.17) after some straightforward derivations.

This concludes the proof of Proposition 2.14. □

D.9 Proof of the converse part of Proposition 2.15

Let $(R_A, R_C, D, \Delta) \in \mathcal{R}^*_{\text{Gaussian}}$ and $\varepsilon > 0$. There exists an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) such that:

$$\begin{aligned} \mathbb{E}\big[d\big(A^n, g(f_A(A^n), f_C(C^n))\big)\big] &\leq D + \varepsilon \,, \\ \frac{1}{n}\, h(A^n | f_A(A^n), E^n) = \frac{1}{n}\, h(A^n | f_A(A^n)) &\geq \Delta - \varepsilon \,. \end{aligned} \tag{D.18}$$

Denote by $J = f_A(A^n)$ and $K = f_C(C^n)$ the messages transmitted by Alice and Charlie, respectively.

D.9.1 Rates

The rate at Alice verifies the following sequence of inequalities:

$$\begin{aligned} n(R_A + \varepsilon) &\geq H(J) \\ &\geq I(J; A^n | K) \\ &= h(A^n | K) - h(A^n | JK) \,. \end{aligned}$$

We now study each term of the r.h.s. of the above equation. First, note that from the Gaussian distribution of (A, C) and $K = f_C(C^n)$, there exists random variables $N_{A,i} \sim \mathcal{N}(0, 1-\rho_C^2)$, independent of C^n (and hence of K) such that $A_i = \rho_C C_i + N_{A,i}$, for each $i \in \{1, \ldots, n\}$. The conditional entropy power inequality (EPI) thus yields (see Lemma C.5):

$$\begin{aligned} 2^{\frac{2}{n} h(A^n|K)} &\geq 2^{\frac{2}{n} h(\rho_C C^n | K)} + 2^{\frac{2}{n} h(N_A^n | K)} \\ &= \rho_C^2\, 2^{\frac{2}{n} h(C^n|K)} + 2\pi e (1 - \rho_C^2) \,. \end{aligned} \tag{D.19}$$

On the other hand, the rate at Charlie can be lower bounded as follows:

$$\begin{aligned} n(R_C + \varepsilon) &\geq H(K) \\ &= I(K; C^n) \\ &= h(C^n) - h(C^n | K) \,. \end{aligned}$$

Equation (D.19) thus yields

$$\begin{aligned} 2^{\frac{2}{n} h(A^n|K)} &\geq \rho_C^2\, 2^{\frac{2}{n}(h(C^n) - n(R_C + \varepsilon))} + 2\pi e (1 - \rho_C^2) \\ &= \rho_C^2\, 2\pi e\, 2^{-2(R_C + \varepsilon)} + 2\pi e (1 - \rho_C^2) \,. \end{aligned}$$

Term $h(A^n|JK)$ can be easily upper bounded:

$$\begin{aligned} h(A^n|JK) &\overset{(a)}{=} \sum_{i=1}^{n} h(A_i|JKA^{i-1}) \\ &\overset{(b)}{\leq} \sum_{i=1}^{n} h(A_i|J,K) \\ &\leq \sum_{i=1}^{n} \frac{1}{2}\log\left(2\pi e\,\mathrm{Var}\left[A_i|J,K\right]\right) \\ &\overset{(c)}{\leq} \sum_{i=1}^{n} \frac{1}{2}\log\left(2\pi e\,\mathbb{E}(A_i - g_i(J,K))^2\right) \\ &\overset{(d)}{\leq} \frac{n}{2}\log\left(\frac{2\pi e}{n}\sum_{i=1}^{n}\mathbb{E}(A_i - g_i(J,K))^2\right) \\ &\overset{(e)}{\leq} \frac{n}{2}\log\left(2\pi e(D+\varepsilon)\right)\ , \end{aligned}$$

where

- step (a) follows from the chain rule for conditional entropy,
- step (b) from the fact that conditioning reduces the entropy,
- step (c) from the fact $\mathrm{Var}\left[A_i|J,K\right]$ is the minimum mean square error (over all possible estimators of A_i), for each $i \in \{1,\ldots,n\}$,
- step (d) from the fact that function $\log(\cdot)$ is concave, and Jensen inequality,
- step (e) from the distortion constraint (D.18).

Putting everything together, we proved that

$$\begin{aligned} n(R_A+\varepsilon) &\geq h(A^n|K) - h(A^n|JK) \\ &\geq \frac{n}{2}\log\left(\rho_C^2\, 2\pi e\, 2^{-2(R_C+\varepsilon)} + 2\pi e(1-\rho_C^2)\right) - \frac{n}{2}\log\left(2\pi e(D+\varepsilon)\right) \\ &= \frac{n}{2}\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2(R_C+\varepsilon)}}{D+\varepsilon}\right)\ . \end{aligned}$$

D.9.2 Equivocation rate at Eve

The above argument also provides an upper bound on the equivocation rate:

$$\begin{aligned} n(\Delta-\varepsilon) &\leq h(A^n) - H(J) \\ &\leq \frac{n}{2}\log\left(2\pi e\right) - \frac{n}{2}\log\left(\frac{1-\rho_C^2+\rho_C^2\,2^{-2(R_C+\varepsilon)}}{D+\varepsilon}\right)\ . \end{aligned}$$

This concludes the proof of the converse part of Proposition 2.15. □

D.10 Proof of the converse part of Proposition 2.16

Let (R_A, D, Δ) be an achievable tuple. From Theorem 2.6, it is straightforward to prove that there exist finite sets $\mathcal{U}$, $\mathcal{V}$, random variables U on $\mathcal{U}$, V on $\mathcal{V}$ such that $U \multimap V \multimap A \multimap (C, E)$ form a Markov chain, and a function $\hat{A}\colon \mathcal{V} \to \mathcal{A}$, verifying

$$\begin{aligned} R_A &\geq \beta\, I(V;A)\ , \\ D &\geq \beta\, \mathbb{E}\big[d(A, \hat{A}(V))\big]\ , \\ \Delta &\leq \beta H(A|V) + (1-\beta)H(A|U) - H(E|U) + h_2(\epsilon)\ . \end{aligned}$$

We now prove that there exist $\nu, \mu \in [0, \frac{1}{2}]$ satisfying the inequalities of Proposition 2.16:

D.10.1 Rate

Random variable A is uniformly distributed on $\{0;1\}$, thus:

$$\begin{aligned} I(V;A) &= H(A) - H(A|V) \\ &= 1 - H(A|V)\ . \end{aligned}$$

Since $0 \leq H(A|V) \leq H(A) = 1$, and function h_2 is a continuous one-to-one mapping from $[0, \frac{1}{2}]$ to $[0,1]$, there exists $\nu \in [0, \frac{1}{2}]$ such that $H(A|V) = h_2(\nu)$, and

$$I(V;A) = 1 - h_2(\nu)\ .$$

D.10.2 Distortion at Bob

Since distortion d is the Hamming distance, we can write:

$$\mathbb{E}\big[d(A, \hat{A}(V))\big] = \Pr\left\{\hat{A}(V) \neq A\right\}\ ,$$

and, from Fano's inequality [31]:

$$h_2\left(\Pr\left\{\hat{A}(V) \neq A\right\}\right) + \Pr\left\{\hat{A}(V) \neq A\right\} \log(\|\mathcal{A}\| - 1) \ \geq\ H(A|V)\ ,$$

i.e.,

$$h_2\left(\Pr\left\{\hat{A}(V) \neq A\right\}\right) \geq h_2(\nu)\ .$$

Function h_2 is increasing on $[0, \frac{1}{2}]$, and $\nu \in [0, \frac{1}{2}]$. The last inequality thus implies

$$\Pr\left\{\hat{A}(V) \neq A\right\} \geq \nu\ .$$

D.10.3 Equivocation rate at Eve

Define random variable $\hat{V}$ on $\{0,1\}$ as the output of a BSC with crossover probability ν and input A. Since A is uniformly distributed on $\{0,1\}$, A is also the output of a BSC with crossover probability ν and input $\hat{V}$. From Mrs. Gerber's lemma (see Lemma C.2), we can write, for each $u \in \mathcal{U}$:

$$H(A|U=u) = h_2\left(\nu \star h_2^{-1}\big(H(\hat{V}|U=u)\big)\right) ,$$

and hence,

$$H(A|U) = \sum_{u\in\mathcal{U}} h_2\left(\nu \star h_2^{-1}\big(H(\hat{V}|U=u)\big)\right) p(u) .$$

Following the same argument, since E is the output of a BSC with crossover probability ϵ and input A, it is also the output of a BSC with crossover probability $\epsilon \star \nu$ and input $\hat{V}$, and:

$$H(E|U) = \sum_{u\in\mathcal{U}} h_2\left((\epsilon \star \nu) \star h_2^{-1}\big(H(\hat{V}|U=u)\big)\right) p(u) .$$

Now, for each $u \in \mathcal{U}$, $0 \le H(\hat{V}|U=u) \le H(\hat{V}) \le 1$, and there exists $\mu_u \in [0, \frac{1}{2}]$ such that $H(\hat{V}|U=u) = h_2(\mu_u)$. Consequently,

$$\begin{aligned}(1-\beta)H(A|U) - H(E|U) &= \sum_{u\in\mathcal{U}} \Big[(1-\beta)\, h_2(\nu \star \mu_u) - h_2(\epsilon \star \nu \star \mu_u)\Big] p(u) \\ &\le (1-\beta)\, h_2(\nu \star \mu) - h_2(\epsilon \star \nu \star \mu) ,\end{aligned}$$

where $\mu = \mu_{u^*}$ for some $u^* \in \mathcal{U}$.

This concludes the proof of the converse part of Proposition 2.16. □

APPENDIX E

Auxiliary Proofs of Chapter 3

E.1 Proof of Theorem 3.1 (Outer bound)

Let (k, D, Δ) be an achievable tuple, and $\varepsilon > 0$. There exists an (n, m)-code (F, g) s.t.

$$\frac{m}{n} \leq k + \varepsilon \,, \tag{E.1}$$

$$\mathbb{E}\left[d(A^n, g(B^n, Y^m))\right] \leq D + \varepsilon \,, \tag{E.2}$$

$$\frac{1}{n} H(A^n | E^n Z^m) \geq \Delta - \varepsilon \,, \tag{E.3}$$

with channel input X^m as the output of the encoder $F(A^n)$.

From the fact that random variables A_i, B_i, E_i are independent across time and the channel $X \mapsto (Y, Z)$ is memoryless, the joint distribution of $(A^n, B^n, E^n, X^m, Y^m, Z^m)$ can be written as follows, for each $i \in \{1, \ldots, n\}$ and each $j \in \{1, \ldots, m\}$:

$$\begin{aligned} p(a^n, b^n, e^n, x^m, y^m, z^m) = {} & p(a^{i-1}, b^{i-1}, e^{i-1})\, p(a_i, b_i, e_i)\, p(a_{i+1}^n, b_{i+1}^n, e_{i+1}^n) \\ & \times P_F(x^m | a^n)\, p(y^{j-1}, z^{j-1} | x^{j-1})\, p(y_j, z_j | x_j)\, p(y_{j+1}^m, z_{j+1}^m | x_{j+1}^m) \,. \end{aligned}$$

Following the technique described in Appendix B and using the above expression, we can obtain the graph of Figure E.1 that will be used to establish Markov chains.

For each $i \in \{1, \ldots, n\}$ (resp. each $j \in \{1, \ldots, m\}$), define the source (resp. channel) auxiliary random variables U_i, V_i (resp. Q_j, T_j) as

$$U_i = (\quad\quad B_{i+1}^n, E^{i-1}, Z^m) \,, \tag{E.4}$$

$$V_i = (A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1}, Y^m) \,, \tag{E.5}$$

$$Q_j = (\quad B^n, Y^{j-1}, Z_{j+1}^m) \,, \tag{E.6}$$

$$T_j = (A^n, B^n, Y^{j-1}, Z_{j+1}^m) \,. \tag{E.7}$$

Note that $(U_i, V_i) \multimap A_i \multimap (B_i, E_i)$, and $Q_j \multimap T_j \multimap X_j \multimap (Y_j, Z_j)$ form Markov chains (see Figure E.1).

Following the usual technique, we introduce independent random variables K and J, uniformly distributed over the sets $\{1, \ldots, n\}$ and $\{1, \ldots, m\}$, respectively. We also define random variables $A = A_K$, $B = B_K$, $E = E_K$, $U = (K, U_K)$, $V = (K, V_K)$, $X = X_J$, $Y = Y_J$, $Z = Z_J$, $Q = (J, Q_j)$, and $T = (J, T_j)$. $(U, V) \multimap A \multimap (B, E)$ and $Q \multimap T \multimap X \multimap (Y, Z)$ still form Markov chains. (A, B, E), resp. (X, Y, Z), is distributed according to $p(abe)$, resp. $p(xyz)$, i.e., the original distribution of (A_i, B_i, E_i), resp. (X_j, Y_j, Z_j).

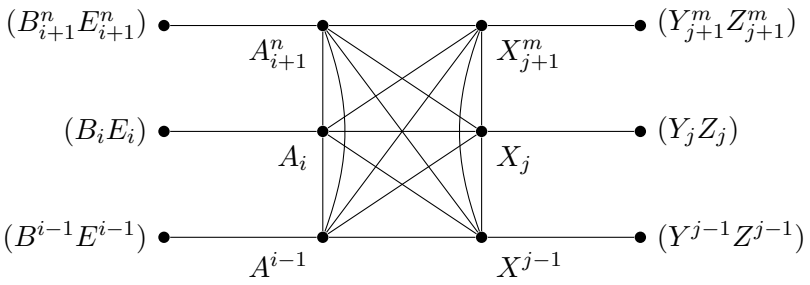


Figure E.1: Outer bound–Graphical representation of distribution $p(a^n b^n e^n x^m y^m z^m)$.

E.1.1 Rate

We first prove the rate inequality (3.1) in Theorem 3.1:

$$
\begin{aligned}
I(A^n;Y^m|B^n) &\overset{(a)}{=} \sum_{i=1}^{n} I(A_i;Y^m|A^{i-1}B^n) \\
&\overset{(b)}{=} \sum_{i=1}^{n} I(A_i;Y^m|A^{i-1}B^nE^{i-1}) \\
&= \sum_{i=1}^{n} \Big[I(A_i;A^{i-1}B^{i-1}B_{i+1}^nE^{i-1}Y^m|B_i) - I(A_i;A^{i-1}B^{i-1}B_{i+1}^nE^{i-1}|B_i) \Big] \\
&\overset{(c)}{=} \sum_{i=1}^{n} I(A_i;A^{i-1}B^{i-1}B_{i+1}^nE^{i-1}Y^m|B_i) \\
&\overset{(d)}{=} \sum_{i=1}^{n} I(A_i;V_i|B_i) \ ,
\end{aligned}
$$

where

- step (a) follows from the chain rule for conditional mutual information,
- step (b) from the Markov chain $(A_i, Y^m) \multimap (A^{i-1}, B^n) \multimap E^{i-1}$ (see Figure E.1),
- step (c) from the independence of random variables A_i, B_i, and E_i across time,
- step (d) from definition (E.5).

We now find an upper bound for the latter quantity:

$$
\begin{aligned}
I(A^n;Y^m|B^n) &\overset{(a)}{=} \sum_{j=1}^{m} I(A^n;Y_j|B^nY^{j-1}) \\
&\overset{(b)}{\leq} \sum_{j=1}^{m} I(A^nB^nY^{j-1}Z_{j+1}^m;Y_j) \\
&\overset{(c)}{\leq} \sum_{j=1}^{m} I(T_j;Y_j) \ ,
\end{aligned}
$$

where

- step (a) follows from the chain rule for conditional mutual information,
- step (b) from the non-negativity of mutual information,
- step (c) from definition (E.7).

Putting all pieces together, we proved that $\sum_{i=1}^{n} I(A_i; V_i|B_i) \leq \sum_{j=1}^{m} I(T_j; Y_j)$. Using random variables K and J, this inequality writes

$$\sum_{i=1}^{n} I(A_K; V_K|B_K, K=i) \leq \sum_{j=1}^{m} I(T_J; Y_J|J=j) \;,$$

i.e.,

$$I(A; V|B) \leq \frac{m}{n}\, I(T; Y) \;. \tag{E.8}$$

E.1.2 Distortion at Bob

Bob reconstructs $g(B^n, Y^m)$. The i-th coordinate of this estimate is

$$g_i(Y^m, B^{i-1}, B_i, B_{i+1}^n) \triangleq \hat{A}_i(V_i, B_i) \;.$$

The component-wise mean distortion at Bob thus writes:

$$\begin{aligned}
\mathbb{E}\big[d(A^n, g(B^n, Y^m))\big] &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_i, \hat{A}_i(V_i, B_i))\right] \\
&= \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[d(A_K, \hat{A}_K(V_K, B_K)) \;\middle|\; K=i\right] \\
&= \mathbb{E}\left[d(A, \hat{A}(V, B))\right] \;,
\end{aligned} \tag{E.9}$$

where we defined function $\hat{A}$ on $\mathcal{V} \times \mathcal{B}$ by $\hat{A}(V, B) = \hat{A}(K, V_K, B_K) \triangleq \hat{A}_K(V_K, B_K)$.

E.1.3 Equivocation rate at Eve

We expand the equivocation at Eve $H(A^n|E^n Z^m)$ in two ways. First,

$$\begin{aligned}
H(A^n|E^n Z^m) &\overset{(a)}{=} \sum_{i=1}^{n} H(A_i|A_{i+1}^n E^n Z^m) \\
&\overset{(b)}{=} \sum_{i=1}^{n} H(A_i|A_{i+1}^n B_{i+1}^n E^i Z^m) \\
&\overset{(c)}{\leq} \sum_{i=1}^{n} H(A_i|B_{i+1}^n E^i Z^m) \\
&\overset{(d)}{=} \sum_{i=1}^{n} H(A_i|U_i E_i) \;,
\end{aligned}$$

where

- step (a) follows from the chain rule for conditional entropy,
- step (b) from the Markov chain $A_i \multimap (A_{i+1}^n, E^i, Z^m) \multimap (B_{i+1}^n, E_{i+1}^n)$ (see Figure E.1),
- step (c) from the fact that conditioning reduces the entropy,
- step (d) from definition (E.4).

Using random variable K defined above, the equivocation rate at Eve can be upper bounded as follows:

$$\begin{aligned}\frac{1}{n}H(A^n|E^nZ^m) &\leq \frac{1}{n}\sum_{i=1}^{n} H(A_K|U_K E_K, K=i) \\ &= H(A|UE)\,. \end{aligned} \tag{E.10}$$

Then, from standard properties of conditional entropy and mutual information:

$$\begin{aligned} H(A^n|E^nZ^m) &= H(A^n|B^nY^m) + I(A^n;B^nY^m) - I(A^n;E^nZ^m) \\ &= H(A^n|B^nY^m) + I(A^n;Y^m|B^n) + I(A^n;B^n) \\ &\qquad - I(A^n;E^n|Z^m) - I(A^n;Z^m) \\ &\overset{(a)}{=} H(A^n|B^nY^m) + I(A^n;Y^m|B^n) + I(A^nZ^m;B^n) \\ &\qquad - I(A^n;E^n|Z^m) - I(B^nA^n;Z^m) \\ &= \underbrace{H(A^n|B^nY^m) + I(A^n;B^n|Z^m) - I(A^n;E^n|Z^m)}_{\Delta_s} \\ &\qquad + \underbrace{I(A^n;Y^m|B^n) - I(A^n;Z^m|B^n)}_{\Delta_c}\,, \end{aligned}$$

where step (a) follows from the Markov chain $B^n \multimap A^n \multimap Z^m$.

From definitions (E.4), (E.5) and following the argument of the proof of the converse part of Theorem 2.6 (given in Appendix D.5), we can prove that

$$\begin{aligned}\Delta_s &= \sum_{i=1}^{n}\Big[H(A_i|V_iB_i) + I(A_i;B_i|U_i) - I(A_i;E_i|U_i)\Big] \\ &= \sum_{i=1}^{n}\Big[H(A_i|U_iE_i) - \Big(I(A_i;V_i|B_i) - I(A_i;U_i|B_i)\Big)\Big]\,. \end{aligned}$$

From definitions (E.6), (E.7) and following the argument of [32, Section V], [90, Section 2.4], we can prove that

$$\Delta_c = \sum_{j=1}^{m}\Big[I(T_j;Y_j|Q_j) - I(T_j;Z_j|Q_j)\Big]\,.$$

Gathering the above equation, using variables K, J, and new source-channel variables, the equivocation rate at Eve writes:

$$\frac{1}{n}H(A^n|E^nZ^m) = H(A|UE) - \Big[I(A;V|B) - I(A;U|B) - \frac{m}{n}\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big] . \quad \text{(E.11)}$$

E.1.4 End of proof

Inequalities (E.8)–(E.11) only involve *marginal* distributions of auxiliary variables $p(uv|a)$ and $p(qtx)$. Consequently, we can define new variables $\tilde{U}$, $\tilde{V}$, $\tilde{Q}$, $\tilde{T}$, $\tilde{X}$, with identical marginal distributions $p(uv|a)$ and $p(qtx)$ (and hence verifying inequalities (E.8)–(E.11)) such that the (global) joint distribution writes $p(uvqtabexyz) = p(uv|a)p(abe)\,p(q|t)p(t)\,p(x|t)p(yz|x)$ i.e., source and channel variables are independent.

Gathering inequalities (E.8)–(E.11) and (E.1)–(E.3), we then proved that, for each achievable tuple (k, D, Δ) and each $\varepsilon > 0$, there exist random variables U, V, Q, T, X with joint distribution $p(uvqtabexyz) = p(uv|a)p(abe)p(q|t)p(t)p(x|t)p(yz|x)$, and a function $\hat{A}$ such that

$$\begin{aligned} &I(A;V|B) \le (k+\varepsilon)I(T;Y) , \\ &\quad D + \varepsilon \ge \mathbb{E}\big[d(A, \hat{A}(V,B))\big] , \\ &\quad \Delta - \varepsilon \le H(A|UE) - \Big[I(V;A|B) - I(U;A|B) - (k+\varepsilon)\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+ , \end{aligned}$$

i.e., $(k+\varepsilon, D+\varepsilon, \Delta-\varepsilon) \in \mathcal{R}_{\text{out}}$. Letting ε tend to zero then proves Theorem 3.1. □

E.2 Proof of the converse part of Proposition 3.6

Let $(k = 1, D = 0, \Delta) \in \mathcal{R}_{\text{digital}}$ i.e., such that there exist random variables U, V, Q, T, X with joint distribution $p(uvqtaexyz) = p(u|v)p(v|a)p(ae)p(q|t)p(tx)p(yz|x)$, and a function $\hat{A}$, verifying

$$\begin{aligned} &I(U;A|B) \le I(Q;Y) , \\ &I(V;A|B) \le I(T;Y) , \\ &0 \ge \mathbb{E}\big[d(A, \hat{A}(V,B))\big] , \\ &\Delta \le H(A|UE) - \Big[I(V;A|UB) - \Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+ . \end{aligned}$$

From the assumptions of Section 3.5, we can easily prove the following inequalities:

$$\beta(1 - H(A|U)) \le 1 - H(X|Q) , \quad \text{(E.12)}$$

$$\Delta \le H(A|U) + h_2(\epsilon) - H(E|U) - \Big[\beta H(A|U) - \Big(H(X|Q) - H(Z|Q) + h_2(\zeta)\Big)\Big]_+ . \quad \text{(E.13)}$$

Since $0 \leq H(A|U) \leq H(A) = 1$ and $0 \leq H(X|Q) \leq H(X) \leq 1$, we now introduce two parameters: $u = h_2^{-1}\big(H(A|U)\big)$, $q = h_2^{-1}\big(H(X|Q)\big)$.

Then, from the fact that E is the output of a BSC with crossover probability ϵ and input A, Mrs. Gerber's lemma yields (see Corollary C.3):

$$H(E|U) \geq h_2(\epsilon \star u) \; . \tag{E.14}$$

Similarly, since Z is the output of a BSC with crossover probability ζ and input X:

$$H(Z|Q) \geq h_2(\zeta \star q) \; . \tag{E.15}$$

Gathering (E.12)–(E.15), we obtain

$$\begin{aligned}
&\beta(1 - h_2(u)) \leq 1 - h_2(q) \; , \\
&\Delta \leq h_2(u) + h_2(\epsilon) - h_2(\epsilon \star u) - \Big[\beta h_2(u) - \Big(h_2(q) - h_2(\zeta \star q) + h_2(\zeta)\Big)\Big]_+ \; .
\end{aligned}$$

This proves the converse part of Proposition 3.6. □

E.3 Proof of Lemma 3.9

In this section, we prove Lemma 3.9 following the argument of [91]. In the decoding procedure described in Section 3.7.3, an error occurs in the first step if there exists another admissible codeword $u^n(r_1')$ with $r_1' \neq r_1$. The probability of this event writes

$$\begin{aligned}
P_{d,1} &\triangleq \Pr\left\{\exists\, r_1' \neq r_1 : (u^n(r_1'), B^n, Y^n) \in T_\delta^n(U,B,Y)\right\} \\
&\leq \sum_{r_1'=1}^{2^{nR_1}} \Pr\left\{r_1 \neq r_1', (u^n(r_1'), B^n, Y^n) \in T_\delta^n(U,B,Y)\right\} \\
&= \sum_{r_1'=1}^{2^{nR_1}} \sum_{a^n} p(a^n) \Pr\left\{r_1 \neq r_1', (u^n(r_1'), B^n, Y^n) \in T_\delta^n(U,B,Y) \;\middle|\; A^n = a^n\right\} \; .
\end{aligned} \tag{E.16}$$

We now study each term of the above summation: For each r_1', and each a^n,

$$\begin{aligned}
&\Pr\left\{r_1 \neq r_1', (u^n(r_1'), B^n, Y^n) \in T_\delta^n(U,B,Y) \;\middle|\; A^n = a^n\right\} \\
&\quad\leq \Pr\left\{(u^n(r_1'), B^n, Y^n) \in T_\delta^n(U,B,Y) \;\middle|\; A^n = a^n, r_1 \neq r_1'\right\} \\
&\quad= \sum_{(u^n,b^n,y^n) \in T_\delta^n(U,B,Y)} \Pr\left\{u^n(r_1') = u^n, B^n = b^n, Y^n = y^n \;\middle|\; A^n = a^n, r_1 \neq r_1'\right\} \\
&\quad= \sum_{(u^n,b^n,y^n) \in T_\delta^n(U,B,Y)} \Pr\left\{u^n(r_1') = u^n \;\middle|\; A^n = a^n, r_1 \neq r_1'\right\} \\
&\qquad\qquad \times \Pr\left\{B^n = b^n, Y^n = y^n \;\middle|\; A^n = a^n, r_1 \neq r_1'\right\} \; .
\end{aligned} \tag{E.17}$$

For each r'_1, and each a^n, according to the encoding procedure described in Section 3.7.2,

$$\begin{aligned}\Pr\left\{r_1 = r'_1 \,\middle|\, A^n = a^n\right\} &= \Pr\left\{\left(\bigcap_{k=1}^{r'_1-1}\left\{u^n(k) \notin T_\delta^n(U|a^n)\right\}\right) \cap \left\{u^n(r'_1) \in T_\delta^n(U|a^n)\right\}\right\} \\ &\leq \Pr\left\{u^n(r'_1) \in T_\delta^n(U|a^n)\right\} \\ &\leq 2^{-n(I(U;A)-\eta_n)}\,,\end{aligned}$$

where the last inequality holds for some sequence $\eta_n \xrightarrow[n\to\infty]{} 0$ (see Lemma A.4 in Appendix A) from the fact that the codewords are uniformly distributed over $T_\delta^n(U)$, independent of the source, and $a^n \in T_\delta^n(A)$. From this inequality, there exists $\kappa < 1$ such that, for some sufficiently large n,

$$\Pr\left\{r_1 = r'_1 \,\middle|\, A^n = a^n\right\} \leq \kappa\,. \tag{E.18}$$

The above upper bound yields the following inequality, for each u^n, r'_1, and a^n:

$$\begin{aligned}&\Pr\left\{u^n(r'_1) = u^n \,\middle|\, A^n = a^n, r_1 \neq r'_1\right\} \\ &\qquad = \Pr\left\{u^n(r'_1) = u^n \,\middle|\, A^n = a^n\right\} \frac{\Pr\left\{r_1 \neq r'_1 \,\middle|\, A^n = a^n, u^n(r'_1) = u^n\right\}}{1 - \Pr\left\{r_1 = r'_1 \,\middle|\, A^n = a^n\right\}} \\ &\qquad \leq \frac{\Pr\left\{u^n(r'_1) = u^n\right\}}{1-\kappa}\,,\end{aligned} \tag{E.19}$$

where the above equation follows from (E.18) and the fact that $u^n(r'_1)$ and A^n are independent.

Plugging (E.19) into (E.17) yields, for each r'_1, and each a^n,

$$\begin{aligned}&\Pr\left\{r_1 \neq r'_1, (u^n(r'_1), B^n, Y^n) \in T_\delta^n(U,B,Y) \,\middle|\, A^n = a^n\right\} \\ &\qquad \leq \sum_{(u^n,b^n,y^n)\in T_\delta^n(U,B,Y)} \frac{\Pr\left\{u^n(r'_1) = u^n\right\}}{1-\kappa} \\ &\qquad\qquad \times \Pr\left\{B^n = b^n, Y^n = y^n \,\middle|\, A^n = a^n, r_1 \neq r'_1\right\}\,.\end{aligned} \tag{E.20}$$

From (E.18) once again, the last term in the r.h.s. of the above equation can be upper bounded as follows, for each r'_1, each a^n, and each $(b^n, y^n) \in T_\delta^n(B,Y)$:

$$\begin{aligned}\Pr\left\{B^n = b^n, Y^n = y^n \,\middle|\, A^n = a^n, r_1 \neq r'_1\right\} &= \frac{\Pr\left\{B^n = b^n, Y^n = y^n, r_1 \neq r'_1 \,\middle|\, A^n = a^n\right\}}{\Pr\left\{r_1 \neq r'_1 \,\middle|\, A^n = a^n\right\}} \\ &\leq \frac{\Pr\left\{B^n = b^n, Y^n = y^n \,\middle|\, A^n = a^n\right\}}{1-\kappa}\,.\end{aligned} \tag{E.21}$$

Gathering (E.16), (E.20) and (E.21), we obtain, from the fact that the codewords are identically distributed,

$$P_{d,1} \leq \frac{2^{nR_1}}{(1-\kappa)^2} \sum_{(u^n,b^n,y^n)\in T_\delta^n(U,B,Y)} \Pr\{u^n(1)=u^n\} \Pr\{B^n=b^n, Y^n=y^n\} \ .$$

Finally, from the joint typicality lemma (Lemma A.4 in Appendix A), there exists a sequence $\eta'_n \xrightarrow[n\to\infty]{} 0$ such that

$$P_{d,1} \leq \frac{2^{nR_1}}{(1-\kappa)^2} \, 2^{-n(I(U;BY)-\eta'_n)} \ .$$

This proves Lemma 3.9. □

E.4 Proof of Proposition 3.10

In this section, we prove a sequence of lemmas which together prove Proposition 3.10. To that end, using auxiliary variables (3.26)–(3.28), we show that any tuple (D, D_E) verifying conditions (3.30)–(3.32) in Proposition 3.10 lies in region $\mathcal{R}^P_{\text{hybrid}}$.

E.4.1 Conditional covariance of Gaussian variables

The following lemma can be found in [135, Appendix A.2]:

Lemma E.1 (Conditional covariance matrix of Gaussian vectors)**.** *Let P, Q be two jointly Gaussian random vectors with covariance matrix*

$$\Gamma_{PQ} = \begin{bmatrix} A & C^{\mathrm{T}} \\ C & B \end{bmatrix} \ .$$

Then the conditional covariance matrix $\Gamma_{(P|Q)}$ of P given Q verifies the following equality

$$\Gamma_{(P|Q)} = A - CB^{-1}C^{\mathrm{T}} \ . \tag{E.22}$$

From the above lemma, we can easily derive the following corollary, which gives the conditional variance for two scalar Gaussian random variables.

Corollary E.2 (Conditional variance of Gaussian variables)**.** *Let P and Q be two jointly Gaussian random variables. Then*

$$Var\,[P|Q] = \frac{\det \Gamma_{PQ}}{Var\,[Q]} \ . \tag{E.23}$$

E.4.2 Preliminary lemmas

Lemma E.3. *With definition* (3.27),

$$I(V;A) = \frac{1}{2}\log\left(1+\frac{\alpha^2}{\gamma^2}\right) . \tag{E.24}$$

Proof. From definition (3.27), the covariance matrix of (A,V) is given by

$$\Gamma_{AV} = \begin{bmatrix} 1 & \alpha \\ \alpha & \alpha^2+\gamma^2 \end{bmatrix} .$$

Lemma E.3 then directly follows from equality

$$I(V;A) = \frac{1}{2}\log\left(\frac{\text{Var}\,[A]}{\text{Var}\,[A|V]}\right) ,$$

and Corollary E.2. □

Lemma E.4. *With definitions* (3.27), (3.28),

$$Var\,[V|BY] = \gamma^2\,\frac{1+\frac{1}{P_B}+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2}{1+\frac{1}{P_B}+\frac{P}{P_Y}\left(1+\frac{\gamma^2}{P_B}\right)} . \tag{E.25}$$

Proof. From definitions (3.27), (3.28), the covariance matrix of (V,B,Y) is given by

$$\Gamma_{VBY} = \begin{bmatrix} \alpha^2+\gamma^2 & \alpha & (\alpha\beta-\gamma^2)\sqrt{P} \\ \alpha & 1+P_B & \beta\sqrt{P} \\ (\alpha\beta-\gamma^2)\sqrt{P} & \beta\sqrt{P} & P+P_Y \end{bmatrix} .$$

This equation comes from the following sequence of equalities, using (3.29):

$$\begin{aligned} \mathbb{E}[VY] &= \mathbb{E}[VX] \\ &= \big((\alpha+\beta)\mathbb{E}[VA] - \text{Var}\,[V]\,\big)\sqrt{P} \\ &= \left(\alpha\beta-\gamma^2\right)\sqrt{P} . \end{aligned}$$

Lemma E.4 then follows from Lemma E.1 after some straightforward manipulations. □

Letting P_B tend to zero in the above lemma yields the following corollary (which can also been proved independently using similar argument):

Corollary E.5. *With definitions* (3.27), (3.28),

$$Var\,[V|AY] = \frac{\gamma^2}{1+\gamma^2\frac{P}{P_Y}} . \tag{E.26}$$

Lemma E.6. *With definitions* (3.27), (3.28),

$$Var\left[A|BY\right] = \frac{1+\gamma^2\frac{P}{P_Y}}{1+\frac{1}{P_B}+\frac{P}{P_Y}\left(1+\frac{\gamma^2}{P_B}\right)} \,. \tag{E.27}$$

Proof. From definitions (3.27), (3.28), the covariance matrix of (A, B, Y) is given by

$$\Gamma_{ABY} = \begin{bmatrix} 1 & 1 & \beta\sqrt{P} \\ 1 & 1+P_B & \beta\sqrt{P} \\ \beta\sqrt{P} & \beta\sqrt{P} & P+P_Y \end{bmatrix} .$$

Lemma E.6 then follows from Lemma E.1 after some straightforward manipulations. □

Lemma E.7. *With definitions* (3.27), (3.28),

$$I(X;Z|E) = \frac{1}{2}\log\left(\frac{1+\frac{1}{P_E}+\frac{P}{P_Z}\left(1+\frac{\gamma^2}{P_E}\right)}{1+\frac{1}{P_E}}\right) \,. \tag{E.28}$$

Proof. Lemma E.7 directly follows from Corollary E.1 together with equality $\text{Var}\left[Y|X\right] = P_Y$, expansion

$$I(X;Z|E) = h(Z|E) - h(Z|X) \,,$$

which comes from the Markov chain $Z \multimap X \multimap E$, and the following expression of the covariance matrix of (Z, E):

$$\Gamma_{ZE} = \begin{bmatrix} P+P_Z & \beta\sqrt{P} \\ \beta\sqrt{P} & 1+P_E \end{bmatrix} .$$

□

E.4.3 End of proof

We now combine the above lemmas to prove that the inequalities (3.16)–(3.19) and (3.25) are verified by variables (3.26)–(3.28) under conditions (3.30)–(3.32).

As a matter of fact, inequality (3.16) is verified with definition (3.26). From (3.28) and (3.33), $X \sim \mathcal{N}(0, P)$ and the power constraint (3.25) is also verified.

E.4.3.1 Proof of (3.17)

From Lemma E.4 and equality $\text{Var}\left[V\right] = \alpha^2 + \gamma^2$, $I(V;BY)$ writes

$$I(V;BY) = \frac{1}{2}\log\left(\left(1+\frac{\alpha^2}{\gamma^2}\right)\frac{1+\frac{1}{P_B}+\frac{P}{P_Y}\left(1+\frac{\gamma^2}{P_B}\right)}{1+\frac{1}{P_B}+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2}\right) \,. \tag{E.29}$$

This equality together with Lemma E.3 and constraint (3.32) proves (3.17).

E.4.3.2 Proof of (3.18)

In the quadratic Gaussian case considered in Section 3.9, distortion measure d is the Euclidean distance on $\mathbb{R}$:

$$\mathbb{E}\big[d(A,\hat{A}(V,B,Y))\big] = \mathbb{E}\left[\big(A-\hat{A}(V,B,Y)\big)^2\right] .$$

Moreover, in the proposed scheme, function $\hat{A}$ is the MMSE estimator of A from (V,B,Y), therefore

$$\mathbb{E}\big[d(A,\hat{A}(V,B,Y))\big] = \mathrm{Var}\left[A|VBY\right] .$$

We now use the Markov chain $V \multimap (A,Y) \multimap B$ to expand the following conditional entropy:

$$h(A|VBY) = h(A|BY) + h(V|AY) - h(V|BY) ,$$

and since the above random variables are jointly Gaussian, this yields

$$\mathbb{E}\big[d(A,\hat{A}(V,B,Y))\big] = \frac{\mathrm{Var}\left[A|BY\right]\mathrm{Var}\left[V|AY\right]}{\mathrm{Var}\left[V|BY\right]} .$$

Gathering Lemmas E.4, E.6 and Corollary E.5, the above equation writes

$$\mathbb{E}\big[d(A,\hat{A}(V,B,Y))\big] = \frac{1}{1+\frac{1}{P_B}+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2} ,$$

and hence (3.18) is verified under constraint (3.30).

E.4.3.3 Proof of (3.19)

From Corollary E.2 with the covariance matrix Γ_{AE} given below, Lemmas E.3 and E.7, we can easily prove the following equality:

$$h(A|E) - I(V;A) - I(X;Z|E) = \frac{1}{2}\log\left(\frac{2\pi e}{\left(1+\frac{\alpha^2}{\gamma^2}\right)\left(1+\frac{1}{P_E}+\frac{P}{P_Z}\left(1+\frac{\gamma^2}{P_E}\right)\right)}\right) . \quad \text{(E.30)}$$

$$\Gamma_{AE} = \begin{bmatrix} 1 & 1 \\ 1 & 1+P_E \end{bmatrix} .$$

Then, letting P_B tend to zero and replacing P_Y by P_Z in (E.29) yields the following equality (which can also been proved independently using argument similar to the one Lemma E.4):

$$I(V;AZ) = \frac{1}{2}\log\left(\left(1+\frac{\alpha^2}{\gamma^2}\right)\left(1+\gamma^2\frac{P}{P_Z}\right)\right) . \quad \text{(E.31)}$$

Inequality (3.19) then follows under constraint (3.31) from (E.29)–(E.31) and definition $D_E = 2^{2\Delta}/(2\pi e)$.

This concludes the proof of Proposition 3.10. □

E.5 Proof of the converse part of Theorem 3.11

Let (D, D_E) be an achievable tuple. From the outer bound $\mathcal{R}_{\text{out}}^{P}$, there exist random variables U, V, Q, T, X with joint distribution $p(uvqtaexyz) = p(uv|a)p(ae)\, p(q|t)p(tx)p(y|x)\, p(z|y)$,[1] and a function $\hat{A}$, verifying

$$\begin{aligned}
&I(V;A) \leq I(T;Y)\,,\\
&D \geq \mathbb{E}\big[d(A,\hat{A}(V))\big]\,,\\
&\Delta \leq h(A|UE) - \Big[I(V;A) - I(U;A) - \Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+\,,\\
&\mathrm{Var}\,[X] \leq P\,,
\end{aligned}$$

where $\Delta = \frac{1}{2}\log(2\pi e\, D_E)$.

From the Markov chain $Q \multimap T \multimap X \multimap Y \multimap Z$, tuple (D, Δ) verifies the following inequalities:

$$I(V;A) \leq I(X;Y)\,, \tag{E.32}$$

$$D \geq \mathbb{E}\big[d(A,\hat{A}(V))\big]\,, \tag{E.33}$$

$$\Delta \leq h(A|UE) - \Big[I(V;A) - I(U;A) - I(X;Y|Z)\Big]_+\,, \tag{E.34}$$

$$\mathrm{Var}\,[X] \leq P\,. \tag{E.35}$$

Moreover, from the proof of Theorem 3.1 (see (E.4), (E.5) in Appendix E.1), we can restrict our attention to auxiliary variables U, V s.t. $U \multimap V \multimap A \multimap E$ form a Markov chain.

We introduce two parameters: $\nu = 2^{2h(A|V)}/(2\pi e)$, $\mu = 2^{2h(A|U)}/(2\pi e)$. From the fact that conditioning reduces the entropy and classical properties of the differential entropy, the above parameters are thus bounded as follows:

$$\nu \leq \mu \leq 1\,. \tag{E.36}$$

We now write (E.32)–(E.35) as functions of these parameters. First, recalling that distortion measure d is the Euclidean distance on $\mathbb{R}$,

$$\mathbb{E}\big[d(A,\hat{A}(V))\big] \geq \mathrm{Var}\,[A|V] \geq \nu\,. \tag{E.37}$$

Then, from the Markov chain $U \multimap A \multimap E$, we write

$$h(A|UE) = h(A|U) - h(E|U) + h(E|A)\,. \tag{E.38}$$

Now, since $E = A + N_E$ with N_E independent of A (and U), the conditional entropy power inequality yields (see Lemma C.5):

$$2^{2h(E|U)} \geq 2^{2h(A|U)} + 2^{2h(N_E)}\,. \tag{E.39}$$

[1] Since it is assumed that $P_Y < P_Z$, according to Remark 3.2, the Markov chain $X \multimap Y \multimap Z$ can be assumed here without loss of generality.

Gathering (E.38) and (E.39), we obtain:

$$\begin{aligned} h(A|UE) &\leq h(A|U) - \frac{1}{2}\log\left(2^{2h(A|U)} + 2^{2h(N_E)}\right) + h(E|A) \\ &= \frac{1}{2}\log\left(\frac{1}{\frac{1}{2^{2h(A|U)}} + \frac{1}{2^{2h(N_E)}}}\right) \\ &= \frac{1}{2}\log\left(\frac{2\pi e}{\frac{1}{\mu} + \frac{1}{P_E}}\right) . \end{aligned} \tag{E.40}$$

From the Markov chain $X \multimap Y \multimap Z$, there exists a random variable $\widetilde{N}_Z \sim \mathcal{N}(0, P_Z - P_Y)$, independent of Y such that $Z = Y + \widetilde{N}_Z$. Then the EPI yields (see Lemma C.4):

$$2^{2h(Z)} \geq 2^{2h(Y)} + 2^{2h(\widetilde{N}_Z)} .$$

From the latter equation and inequality $\mathrm{Var}\,[Y] \leq P + P_Y$,

$$\begin{aligned} I(X;Y|Z) &= h(Y) - h(Y|X) - h(Z) + h(Z|X) \\ &\leq h(Y) - h(N_Y) - \frac{1}{2}\log\left(2^{2h(Y)} + 2^{2h(\widetilde{N}_Z)}\right) + h(N_Z) \\ &\leq \frac{1}{2}\log\left(\frac{1}{1 + \frac{P_Z - P_Y}{P + P_Y}}\,\frac{P_Z}{P_Y}\right) \\ &= \frac{1}{2}\log\left(\frac{1 + \frac{P}{P_Y}}{1 + \frac{P}{P_Z}}\right) . \end{aligned} \tag{E.41}$$

Gathering the above equations, tuple (D, D_E) verifies the following inequalities:

$$\begin{aligned} &\nu \leq \mu \leq 1 , \\ &\frac{1}{\nu} \leq 1 + \frac{P}{P_Y} , \\ &D \geq \nu , \\ &D_E \leq \frac{1}{\frac{1}{\mu} + \frac{1}{P_E}} , \\ &D_E \leq \frac{1}{\frac{1}{\mu} + \frac{1}{P_E}}\,\frac{\nu}{\mu}\,\frac{1 + \frac{P}{P_Y}}{1 + \frac{P}{P_Z}} . \end{aligned}$$

Eliminating parameter ν,

$$\frac{1}{1+\frac{P}{P_Y}} \leq \mu \leq 1 \,, \tag{E.42}$$

$$\frac{1}{1+\frac{P}{P_Y}} \leq D \,, \tag{E.43}$$

$$D_E \leq \frac{1}{\frac{1}{\mu}+\frac{1}{P_E}} \,, \tag{E.44}$$

$$D_E \leq \frac{1}{\frac{1}{\mu}+\frac{1}{P_E}} \frac{1+\frac{P}{P_Y}}{1+\frac{P}{P_Z}} \,, \tag{E.45}$$

$$D_E \leq \frac{1}{\frac{1}{\mu}+\frac{1}{P_E}} \frac{1+\frac{P}{P_Y}}{1+\frac{P}{P_Z}} \frac{D}{\mu} \,. \tag{E.46}$$

Since we assumed that $P_Y < P_Z$, (E.45) is directly verified under constraint (E.44). Inequalities (E.44) and (E.46) are identical at point $\mu = \mu^* \triangleq D \frac{1+\frac{P}{P_Y}}{1+\frac{P}{P_Z}}$, and then write

$$D_E \leq \frac{1}{\frac{1}{D}\frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}+\frac{1}{P_E}} \,.$$

This proves the converse part of Theorem 3.11. □

E.6 Proof of the direct part of Theorem 3.11

Letting P_B tend to infinity, (3.30)–(3.32) write

$$D \geq \frac{1}{1+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2} \,, \tag{E.47}$$

$$D_E \leq \frac{1}{1+\frac{1}{P_E}+\frac{P}{P_Z}\left(1+\frac{\gamma^2}{P_E}\right)} \cdot \min\left\{ \frac{1+\frac{P}{P_Y}}{1+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2} ; 1+\gamma^2\frac{P}{P_Z} \right\} \,, \tag{E.48}$$

$$\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2 \leq \frac{P}{P_Y} \,. \tag{E.49}$$

We then check that these equations are verified with definitions (3.36), (3.37) under constraint (3.35). Recall that we consider here any distortion level $D \in \left[\frac{1}{1+\frac{P}{P_Y}}, \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}\right]$.

E.6.1 Proof of (E.47)

From definitions (3.36), (3.37), on one hand:

$$\alpha^2 = \left(\frac{\gamma^2 \sqrt{\frac{1}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right)} - \beta\gamma^2 \frac{P}{P_Y}}{1 + \gamma^2 \frac{P}{P_Y}} \right)^2$$
$$= \gamma^4 \frac{\frac{1}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right) + \beta^2 \left(\frac{P}{P_Y}\right)^2 - 2\beta \frac{P}{P_Y} \sqrt{\frac{1}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right)}}{\left(1 + \gamma^2 \frac{P}{P_Y}\right)^2} ,$$

on the other hand:

$$(\alpha + \beta)^2 = \frac{\beta^2 + \frac{\gamma^4}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right) + 2\beta\gamma^2 \sqrt{\frac{1}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right)}}{\left(1 + \gamma^2 \frac{P}{P_Y}\right)^2} .$$

The denominator in (E.47) thus writes

$$1 + \frac{\alpha^2}{\gamma^2} + \frac{P}{P_Y}(\alpha + \beta)^2 = 1 + \frac{\frac{\gamma^2}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right) + \gamma^2\beta^2 \left(\frac{P}{P_Y}\right)^2 + \beta^2 \frac{P}{P_Y} + \frac{\gamma^4}{D}\frac{P}{P_Y}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right)}{\left(1 + \gamma^2 \frac{P}{P_Y}\right)^2}$$
$$= 1 + \frac{\frac{\gamma^2}{D}\left(\frac{P}{P_Y} - \frac{P}{P_Z}\right) + \beta^2 \frac{P}{P_Y}}{1 + \gamma^2 \frac{P}{P_Y}}$$
$$= \frac{1 + \frac{P}{P_Y} + \frac{\gamma^2}{D}\frac{P}{P_Y} - \frac{\gamma^2}{D}\frac{P}{P_Z}}{1 + \gamma^2 \frac{P}{P_Y}} , \tag{E.50}$$

where the last equality follows from (3.33).

Now, from definitions (3.33), (3.37):

$$1 + \gamma^2 \frac{P}{P_Z} = D\left(1 + \frac{P}{P_Y}\right) , \tag{E.51}$$

and hence (E.50) writes

$$1 + \frac{\alpha^2}{\gamma^2} + \frac{P}{P_Y}(\alpha + \beta)^2 = \frac{\frac{1}{D} + \frac{\gamma^2}{D}\frac{P}{P_Y}}{1 + \gamma^2 \frac{P}{P_Y}}$$
$$= \frac{1}{D} . \tag{E.52}$$

This proves (E.47).

E.6.2 Proof of (E.48)

First, from (E.51) and (E.52), the two arguments of the $\min\{\cdot\,;\cdot\}$ in (E.48) are equal:

$$\frac{1+\frac{P}{P_Y}}{1+\frac{\alpha^2}{\gamma^2}+\frac{P}{P_Y}(\alpha+\beta)^2} = D\left(1+\frac{P}{P_Y}\right)$$
$$= 1+\gamma^2\,\frac{P}{P_Z}$$

Then, from (E.51) once again, the first term in the r.h.s. of (E.48) writes

$$\frac{1}{1+\frac{1}{P_E}+\frac{P}{P_Z}\left(1+\frac{\gamma^2}{P_E}\right)} = \frac{1}{1+\frac{P}{P_Z}+\frac{D}{P_E}\left(1+\frac{P}{P_Y}\right)}\,,$$

and since (3.35) writes, for $D \leq \frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}$,

$$D_E \leq \frac{1}{\frac{1}{D}\cdot\frac{1+\frac{P}{P_Z}}{1+\frac{P}{P_Y}}+\frac{1}{P_E}}\,,$$

this proves (E.48).

E.6.3 Proof of (E.49)

Inequality (E.49) directly follows from (E.52) and $D \geq \frac{1}{1+\frac{P}{P_Y}}$.

This concludes the proof of the direct part of Theorem 3.11. □

E.7 Proof of the converse part of Proposition 3.12

Let $(D, D_E) \in \mathcal{R}^P_{\text{digital}}$ i.e., such that there exist random variables U, V, Q, T, X, and a function $\hat{A}$, with joint distribution $p(uvqtaexyz) = p(u|v)p(v|a)p(ae)p(q|t)p(tx)p(y|x)$ $p(z|y)$,[2] and verifying

$$I(U;A) \leq I(Q;Y)\,,$$
$$I(V;A) \leq I(T;Y)\,,$$
$$D \geq \mathbb{E}\big[d(A,\hat{A}(V))\big]\,,$$
$$\Delta \leq h(A|UE) - \Big[I(V;A|U) - \Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+\,,$$
$$\text{Var}\,[X] \leq P\,,$$

where $\Delta = \frac{1}{2}\log(2\pi e\, D_E)$.

[2] As in Appendix E.5, since $P_Y < P_Z$, the Markov chain $X \multimap Y \multimap Z$ can be assumed here without loss of generality.

From the Markov chain $Q \multimap T \multimap X \multimap Y \multimap Z$, tuple (D, Δ) verifies the following inequalities:

$$I(U;A) \leq I(Q;Y) \,, \tag{E.53}$$

$$I(V;A) \leq I(X;Y) \,, \tag{E.54}$$

$$D \geq \mathbb{E}\big[d(A, \hat{A}(V))\big] \,, \tag{E.55}$$

$$\Delta \leq h(A|UE) - \Big[I(V;A|U) - I(X;Y|QZ)\Big]_+ \,, \tag{E.56}$$

$$\mathrm{Var}\,[X] \leq P \,. \tag{E.57}$$

We now introduce three parameters: $\nu = 2^{2h(A|V)}/(2\pi e)$, $\mu = 2^{2h(A|U)}/(2\pi e)$, $\zeta = 2^{2h(Y|Q)}/(2\pi e)$. Since $U \multimap V \multimap A \multimap E$ and $Q \multimap X \multimap Y$ form Markov chains, from the fact that conditioning reduces the entropy and inequality $\mathrm{Var}\,[Y] \leq P + P_Y$, the above parameters are bounded as follows:

$$\nu \leq \mu \leq 1 \,, \tag{E.58}$$

$$P_Y \leq \zeta \leq P + P_Y \,. \tag{E.59}$$

We now write (E.53)–(E.57) as functions of these parameters. First, note that (E.37) and (E.40) also hold here. Then, from the Markov chain $Q \multimap X \multimap Y \multimap Z$, there exists a random variable $\widetilde{N}_Z \sim \mathcal{N}(0, P_Z - P_Y)$, independent of (Q, X, Y) such that $Z = Y + \widetilde{N}_Z$. Then the conditional EPI yields (see Lemma C.5):

$$2^{2h(Z|Q)} \geq 2^{2h(Y|Q)} + 2^{2h(\widetilde{N}_Z)} \,.$$

From the latter equation,

$$\begin{aligned} I(X;Y|QZ) &= h(Y|Q) - h(Y|X) - h(Z|Q) + h(Z|X) \\ &\leq h(Y|Q) - h(N_Y) - \frac{1}{2}\log\left(2^{2h(Y|Q)} + 2^{2h(\widetilde{N}_Z)}\right) + h(N_Z) \\ &\leq \frac{1}{2}\log\left(\frac{\zeta}{\zeta + P_Z - P_Y}\frac{P_Z}{P_Y}\right) \,. \end{aligned}$$

Gathering the above equations, tuple (D, D_E) verifies (E.58), (E.59), and

$$\begin{aligned} &\frac{1}{\mu} \leq \frac{P + P_Y}{\zeta} \,, \\ &\frac{1}{\nu} \leq 1 + \frac{P}{P_Y} \,, \\ &D \geq \nu \,, \\ &D_E \leq \frac{1}{\frac{1}{\mu} + \frac{1}{P_E}} \,, \\ &D_E \leq \frac{1}{\frac{1}{\mu} + \frac{1}{P_E}} \frac{\nu}{\mu} \frac{1}{1 + \frac{P_Z - P_Y}{\zeta}} \frac{P_Z}{P_Y} \,. \end{aligned}$$

Eliminating parameters ζ, ν and removing redundant inequalities in the above system prove the converse part of Proposition 3.12. □

E.8 Proof of Proposition 3.13

Consider any distortion level $D \in \left[\frac{1}{1+\frac{P}{P_Y}}, 1\right]$. The analog scheme of Proposition 3.13 then consists in sending a scaled version of the source over the channel:

$$X = \sqrt{\tau}\, A \,, \tag{E.60}$$

where $\tau = P_Y \left(\frac{1}{D} - 1\right)$. Note that, since $D \geq \frac{1}{1+\frac{P}{P_Y}}$, $\mathrm{Var}\,[X] = \tau \leq P$ and the power constraint (3.25) is verified. Bob then simply computes the MMSE estimate $\hat{A}$ of A from Y.

In such an analog scheme, the mean distortion at Bob writes

$$\begin{aligned}
\mathbb{E}\big[d(A, \hat{A}(Y))\big] &= \mathrm{Var}\,[A|Y] \\
&= \frac{P_Y}{\tau + P_Y} \\
&= D \,,
\end{aligned}$$

where the next-to-last equation follows after Corollary E.2 together with the covariance matrix of (A, Y):

$$\Gamma_{AY} = \begin{bmatrix} 1 & \sqrt{\tau} \\ \sqrt{\tau} & \tau + P_Y \end{bmatrix} .$$

The equivocation rate at Eve is $h(A|EZ)$ and quantity D_E then writes

$$\begin{aligned}
D_E &= \mathrm{Var}\,[A|EZ] \\
&= \frac{1}{1 + \frac{1}{P_E} + \frac{\tau}{P_Z}} \\
&= \frac{1}{1 + \frac{1}{P_E} + \left(\frac{1}{D} - 1\right)\frac{P_Y}{P_Z}} \,,
\end{aligned}$$

where the next-to-last equation follows after some straightforward manipulations from Lemma E.1 and the covariance matrix of (A, E, Z):

$$\Gamma_{AEZ} = \begin{bmatrix} 1 & 1 & \sqrt{\tau} \\ 1 & 1 + P_E & \sqrt{\tau} \\ \sqrt{\tau} & \sqrt{\tau} & \tau + P_Y \end{bmatrix} .$$

This proves Proposition 3.13. □

APPENDIX F

Auxiliary Proofs of Chapter 4

F.1 Proof of Lemma 4.6

We write the Taylor-Lagrange expansion of function $y_{-m:u} \mapsto p_1(y_{-m:u})$ at point $\xi_{N,j_{-m:u}}$:

$$p_1(y_{-m:u}) = p_1(\xi_{N,j_{-m:u}}) + \sum_{k=-m}^{u} \nabla_{y_k} p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} (y_k - \xi_{N,j_k}) + \frac{1}{2} \sum_{k,\ell=-m}^{u} (y_k - \xi_{N,j_k})^{\mathrm{T}} \nabla^2_{y_k,y_\ell} p_1(\xi_{N,j_{-m:u}}) (y_\ell - \xi_{N,j_\ell}) + \epsilon_N(y_{-m:u}) , \quad \text{(F.1)}$$

where

$$\epsilon_N(y_{-m:u}) = \frac{1}{6} \sum_{k,\ell,r=-m}^{u} \sum_{h,\bar{\imath},\bar{\jmath}=1}^{d} (y_k^{(h)} - \xi_{N,j_k}^{(h)})(y_\ell^{(\bar{\imath})} - \xi_{N,j_\ell}^{(\bar{\imath})})(y_r^{(\bar{\jmath})} - \xi_{N,j_r}^{(\bar{\jmath})}) \times \frac{\partial^3 p_1}{\partial y_k^{(h)} \, \partial y_\ell^{(\bar{\imath})} \, \partial y_r^{(\bar{\jmath})}} (\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}}) ,$$

for a given $\theta \in [0,1]$ (see [83]).

Plugging expansion (F.1) into (4.19) leads to:

$$\begin{aligned} \frac{\bar{p}_{1,N}(\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} = 1 &+ \sum_{k=-m}^{u} \int_{C_{N,j_k}} \frac{\nabla_{y_k} p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}}}{p_1(\xi_{N,j_{-m:u}})} (y_k - \xi_{N,j_k}) \frac{\mathrm{d}y_k}{V_{N,j_k}} \\ &+ \frac{1}{2} \sum_{k=-m}^{u} \int_{C_{N,j_k}} (y_k - \xi_{N,j_k})^{\mathrm{T}} \frac{\nabla^2_{y_k} p_1(\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} (y_k - \xi_{N,j_k}) \frac{\mathrm{d}y_k}{V_{N,j_k}} \\ &+ \frac{1}{2} \sum_{k \neq \ell} \int_{C_{N,j_k}} \int_{C_{N,j_\ell}} (y_k - \xi_{N,j_k})^{\mathrm{T}} \frac{\nabla^2_{y_k,y_\ell} p_1(\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} (y_\ell - \xi_{N,j_\ell}) \frac{\mathrm{d}y_k}{V_{N,j_k}} \frac{\mathrm{d}y_\ell}{V_{N,j_\ell}} \\ &+ \epsilon_{N,j_{-m:u}} , \end{aligned} \quad \text{(F.2)}$$

where

$$\epsilon_{N,j_{-m:u}} = \int \cdots \int_{C_{N,j_{-m}} \times \cdots \times C_{N,j_u}} \frac{\epsilon_N(y_{-m:u})}{p_1(\xi_{N,j_{-m:u}})} \frac{\mathrm{d}y_{-m:u}}{\prod_{i=-m}^{u} V_{N,j_i}} .$$

We now determine an estimate for this remainder term. For each $y_{-m:u} \in C_{N,j_{-m}} \times \cdots \times C_{N,j_u}$,

$$\frac{\epsilon_N(y_{-m:u})}{p_1(\xi_{N,j_{-m:u}})} = \frac{1}{6} \sum_{k,\ell,r=-m}^{u} \sum_{h,\bar{\imath},\bar{\jmath}=1}^{d} (y_k^{(h)} - \xi_{N,j_k}^{(h)})(y_\ell^{(\bar{\imath})} - \xi_{N,j_\ell}^{(\bar{\imath})})(y_r^{(\bar{\jmath})} - \xi_{N,j_r}^{(\bar{\jmath})}) \\ \times \frac{1}{p_1(\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}})} \frac{\partial^3 p_1}{\partial y_k^{(h)} \, \partial y_\ell^{(\bar{\imath})} \, \partial y_r^{(\bar{\jmath})}} (\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}}) \\ \times \frac{p_1(\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} \,. \quad \text{(F.3)}$$

First, we find a bound for the last factor. To that end, we expand function $z_{-m:u} \mapsto \log p_1(z_{-m:u})$ at point $\xi_{N,j_{-m:u}}$:

$$\log p_1(z_{-m:u}) = \log p_1(\xi_{N,j_{-m:u}}) + \sum_{k=-m}^{u} \nabla_{y_k} \log p_1(\theta' z_{-m:u} + (1-\theta')\xi_{N,j_{-m:u}})^{\mathrm{T}} (z_k - \xi_{N,j_k}) \,,$$

for a given $\theta' \in [0,1]$. From (4.24), the following inequality holds:

$$\left| \log \frac{p_1(z_{-m:u})}{p_1(\xi_{N,j_{-m:u}})} \right| \leq \sum_{k=-m}^{u} \left\| \nabla_{y_k} \log p_1(\theta' z_{-m:u} + (1-\theta')\xi_{N,j_{-m:u}}) \right\| \left\| z_k - \xi_{N,j_k} \right\| \\ \leq C_1 \sum_{k=-m}^{u} \left\| z_k - \xi_{N,j_k} \right\| \,.$$

Applying the above upper bound at point $z_{-m:u} = \theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}}$ and using Assumption 4.3-3), we find

$$\left| \log \frac{p_1(\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})} \right| \leq C_1 (m+1) \frac{C_d}{N^{1/d}} \,,$$

for each $y_{-m:u} \in C_{N,j_{-m}} \times \cdots \times C_{N,j_u}$. According to the definition of sequence $m(N)$ (see (4.23)), the r.h.s. of the above equation vanishes as N tends to infinity. Consequently, the term $\frac{p_1(\theta y_{-m:u} + (1-\theta)\xi_{N,j_{-m:u}})}{p_1(\xi_{N,j_{-m:u}})}$ in (F.3) is bounded. This result together with Assumption 4.4-2) gives the following upper bound:

$$\left| \epsilon_{N,j_{-m:u}} \right| \leq c_T \left(\frac{m+1}{N^{1/d}} \right)^3 \,,$$

for some constant c_T.

Let us now examine the dominant terms of (F.2). Recall that $\xi_{N,j}$ is defined as the centroid of cell $C_{N,j}$:

$$\xi_{N,j} = \int_{C_{N,j}} y \, \frac{\mathrm{d}y}{V_{N,j}} \,.$$

It is straightforward to prove the following two equalities, for any $j \in \{1, \dots, N\}$ and any d-by-d matrix A:

$$\int_{C_{N,j}} (y - \xi_{N,j}) \frac{\mathrm{d}y}{V_{N,j}} = 0 \,,$$
$$\int_{C_{N,j}} (y - \xi_{N,j})^{\mathrm{T}} A \, (y - \xi_{N,j}) \frac{\mathrm{d}y}{V_{N,j}} = \mathrm{Tr}\,(A M_{N,j}) \, V_{N,j}^{2/d} \,.$$

Plugging above identities in (F.2) and recalling that $\zeta_{N,j} = \frac{1}{N V_{N,j}}$ prove Lemma 4.6. □

F.2 Proof of Lemma 4.7

We study each term of the r.h.s. of (4.32). Writing Taylor-Lagrange expansions of the probability densities and using the fact that quantization levels are centroids of the cells, we prove the following three lemmas. Define function V_N on Y by $V_N(y) = V_{N,j}$ whenever $y \in C_{N,j}$.

Lemma F.1. *For each $k \in \{-m, \dots, u\}$, the following equality holds true:*

$$\mathbb{E}_0\Big[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \, (Y_k - Z_{N,k})\Big]$$
$$= \frac{1}{N^{2/d}} \, \mathbb{E}_0\left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} \, \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \, \frac{\nabla_{y_k} p_0(Y_{-m:k-1}, Z_{N,k}, Y_{k+1:u})}{p_0(Y_{-m:u})}\right] + \bar{\epsilon}_{N,k} \,,$$

where $|\bar{\epsilon}_{N,k}| \leq \frac{c_1'}{N^{3/d}}$ for some constant c_1'.

Proof. We expand the expectation:

$$\mathbb{E}_0\Big[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} (Y_k - Z_{N,k})\Big]$$
$$= \sum_{j_{-m:u}} \int \dots \int_{C_{N,j_{-m}} \times \dots \times C_{N,j_u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} \, (y_k - \xi_{N,j_k}) p_0(y_{-m:u}) \, \mathrm{d}y_{-m:u} \,. \quad \text{(F.4)}$$

where $\sum_{j_{-m:u}}$ is a summation over all index vectors $j_{-m:u} \in \{1, \dots, N\}^{u+m+1}$.

For each $j_k \in \{1, \dots, N\}$, we then consider the Taylor-Lagrange expansion of $y_k \mapsto p_0(y_{-m:u})$ at point ξ_{N,j_k}:

$$p_0(y_{-m:u}) = p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})$$
$$+ \nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})^{\mathrm{T}} \, (y_k - \xi_{N,j_k}) + \epsilon_{N,k}(y_{-m:u}) \,, \quad \text{(F.5)}$$

where

$$\epsilon_{N,k}(y_{-m:u}) = (y_k - \xi_{N,j_k})^{\mathrm{T}} \, \nabla_{y_k}^2 p_0(y_{-m:k-1}, \theta y_k + (1-\theta)\xi_{N,j_k}, y_{k+1:u}) \, (y_k - \xi_{N,j_k})$$

for a given $\theta \in [0,1]$. Under Assumption 4.4-2), from the counterparts of (4.24), (4.25) for density p_0 and following the argument of Lemma 4.6 (see Appendix F.1), we can find a bound for this remainder: For each $y_{-m:u} \in C_{N,j_{-m}} \times \cdots \times C_{N,j_u}$,

$$\begin{aligned}
|\epsilon_{N,k}(y_{-m:u})| &\leq \|y_k - \xi_{N,j_k}\|^2 \left\|\nabla^2_{y_k} p_0(y_{-m:k-1}, \theta y_k + (1-\theta)\xi_{N,j_k}, y_{k+1:u})\right\| \\
&= \|y_k - \xi_{N,j_k}\|^2 \left\| \frac{\nabla^2_{y_k} p_0(y_{-m:k-1}, \theta y_k + (1-\theta)\xi_{N,j_k}, y_{k+1:u})}{p_0(y_{-m:k-1}, \theta y_k + (1-\theta)\xi_{N,j_k}, y_{k+1:u})} \right\| \\
&\qquad \times \frac{p_0(y_{-m:k-1}, \theta y_k + (1-\theta)\xi_{N,j_k}, y_{k+1:u})}{p_0(y_{-m:u})}\, p_0(y_{-m:u}) \\
&\leq c\, \|y_k - \xi_{N,j_k}\|^2\, p_0(y_{-m:u})\,, \qquad \text{(F.6)}
\end{aligned}$$

for some constant c.

Plugging expansion (F.5) into (F.4) leads to two dominant terms $D_{N,1}$ and $D_{N,2}$ and a remainder r_N:

$$\mathbb{E}_0\Big[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}} (Y_k - Z_{N,k})\Big] = D_{N,1} + D_{N,2} + r_N\,.$$

We successively study each of them. The first dominant term is

$$\begin{aligned}
D_{N,1} &= \sum_{j_{-m:u}} \int\!\cdots\!\int_{C_{N,j_{-m}} \times \cdots \times C_{N,j_u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} (y_k - \xi_{N,j_k}) \\
&\qquad\qquad \times p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})\, \mathrm{d}y_{-m:u} \\
&= \sum_{j_{-m:u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} \int\!\cdots\!\int_{\{C_{N,j_i}\}_{i\neq k}} \left(\int_{C_{N,j_k}} (y_k - \xi_{N,j_k}) \mathrm{d}y_k \right) \\
&\qquad\qquad \times p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})\, \{\mathrm{d}y_i\}_{i\neq k} \\
&= 0\,,
\end{aligned}$$

where $\{\mathrm{d}y_i\}_{i\neq k}$ stands for $\prod_{i=-m, i\neq k}^{u} \mathrm{d}y_i$. The last equality holds true since we have chosen the quantization level $\xi_{N,j}$ to be the centroid of cell $C_{N,j}$.

The second dominant term is

$$\begin{aligned}
D_{N,2} &= \sum_{j_{-m:u}} \int\!\cdots\!\int_{C_{N,j_{-m}} \times \cdots \times C_{N,j_u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} (y_k - \xi_{N,j_k})(y_k - \xi_{N,j_k})^{\mathrm{T}} \\
&\qquad\qquad \times \nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})\, \mathrm{d}y_{-m:u} \\
&= \sum_{j_{-m:u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} \int\!\cdots\!\int_{\{C_{N,j_i}\}_{i\neq k}} \left(\int_{C_{N,j_k}} (y_k - \xi_{N,j_k})(y_k - \xi_{N,j_k})^{\mathrm{T}} \mathrm{d}y_k \right) \\
&\qquad\qquad \times \nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})\, \{\mathrm{d}y_i\}_{i\neq k} \\
&= \sum_{j_{-m:u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}}\, M_{N,j_k}\, V_{N,j_k}^{1+2/d} \\
&\qquad\qquad \times \int\!\cdots\!\int_{\{C_{N,j_i}\}_{i\neq k}} \nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})\, \{\mathrm{d}y_i\}_{i\neq k}\,. \qquad \text{(F.7)}
\end{aligned}$$

We now write this equality in a simple form. Obviously, under Assumption 4.1-2), we can write

$$\nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u}) = \frac{\nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})}{p_0(y_{-m:u})}\, p_0(y_{-m:u})\,.$$

Note that the above expression is independent of $y_k \in C_{N,j}$, so we can also write

$$\nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u}) = \int_{C_{N,j}} \frac{\nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})}{p_0(y_{-m:u})}\, p_0(y_{-m:u})\, \frac{\mathrm{d}y_k}{V_{N,j}}\,.$$

Equation (F.7) thus becomes

$$\begin{aligned} D_{N,2} &= \sum_{j_{-m:u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}}\, M_{N,j_k}\, V_{N,j_k}^{2/d} \\ &\qquad \times \int\!\cdots\!\int_{\{C_{N,j_i}\}} \frac{\nabla_{y_k} p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u})}{p_0(y_{-m:u})}\, p_0(y_{-m:u})\, \mathrm{d}y_{-m:u} \\ &= \frac{1}{N^{2/d}}\, \mathbb{E}_0\left[\nabla_{y_k} \log p_1(Z_{N,-m:u})^{\mathrm{T}}\, \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}}\, \frac{\nabla_{y_k} p_0(Y_{-m:k-1}, Z_{N,k}, Y_{k+1:u})}{p_0(Y_{-m:u})}\right], \end{aligned}$$

where the last line comes from $\zeta_{N,j} = \frac{1}{NV_{N,j}}$.

We complete the proof with a bound on the remainder term:

$$\begin{aligned} |r_N| &= \left| \sum_{j_{-m:u}} \int\!\cdots\!\int_{C_{N,j_{-m}} \times \cdots \times C_{N,j_u}} \nabla_{y_k} \log p_1(\xi_{N,j_{-m:u}})^{\mathrm{T}} (y_k - \xi_{N,j_k})\, \epsilon_{N,k}(y_{-m:u})\, \mathrm{d}y_{-m:u} \right| \\ &\overset{(a)}{\leq} C_1\, c \int\!\cdots\!\int \|y_k - \xi_N(y_k)\|^3\; p_0(y_{-m:u})\, \mathrm{d}y_{-m:u} \\ &\overset{(b)}{\leq} C_1\, c \left(\frac{C_d}{N^{1/d}}\right)^3 = \frac{c_1'}{N^{3/d}}\,, \end{aligned}$$

where inequality (a) is obtained from (4.24), (F.6), and (b) is a consequence of Assumption 4.3-3).

Putting all pieces together proves Lemma F.1. □

Lemma F.2. *There exists a constant c_2' such that, for each $k \neq \ell \in \{-m, \ldots, u\}$,*

$$\mathbb{E}_0\Big[(Y_k - Z_{N,k})^{\mathrm{T}}\, \nabla^2_{y_k, y_\ell} \log p_1(Z_{N,-m:u})\, (Y_\ell - Z_{N,\ell})\Big] \leq \frac{c_2'}{N^{3/d}}\,.$$

Proof. For each $k \neq \ell$, we expand the expectation:

$$\begin{aligned} &\mathbb{E}_0\left[(Y_k - Z_{N,k})^{\mathrm{T}}\, \nabla^2_{y_k, y_\ell} \log p_1(Z_{N,-m:u})\, (Y_\ell - Z_{N,\ell})\right] \\ &\qquad = \sum_{j_{-m:u}} \int\!\cdots\!\int_{C_{N,j_{-m}} \times \cdots \times C_{N,j_u}} (y_k - \xi_{N,j_k})^{\mathrm{T}}\, \nabla^2_{y_k, y_\ell} \log p_1(\xi_{N,j_{-m:u}}) \\ &\qquad\qquad \times (y_\ell - \xi_{N,j_\ell})\, p_0(y_{-m:u})\, \mathrm{d}y_{-m:u} \end{aligned} \tag{F.8}$$

and consider the expansion of $y_k \mapsto p_0(y_{-m:u})$ at point ξ_{N,j_k}:

$$p_0(y_{-m:u}) = p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u}) + \epsilon'_{N,k}(y_{-m:u}) \,, \tag{F.9}$$

where, from the counterpart of (4.24) for density p_0 and following the argument leading to (F.6), $\left|\epsilon'_{N,k}(y_{-m:u})\right| \leq c' \, \|y_k - \xi_{N,j_k}\| \, p_0(y_{-m:u})$ for some constant c'.

Plugging expansion (F.9) into (F.8) leads to a dominant term and a remainder. The dominant term is

$$\begin{aligned}
&\sum_{j_{-m:u}} \int\cdots\int_{C_{N,j_{-m}}\times\cdots\times C_{N,j_u}} (y_k - \xi_{N,j_k})^{\mathrm{T}} \, \nabla^2_{y_k,y_\ell} \log p_1(\xi_{N,j_{-m:u}}) \, (y_\ell - \xi_{N,j_\ell}) \\
&\qquad\qquad \times p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u}) \, \mathrm{d}y_{-m:u} \\
&= \sum_{j_{-m:u}} \int\cdots\int_{\{C_{N,j_i}\}_{i\neq k}} \left(\int_{C_{N,j_k}} (y_k - \xi_{N,j_k}) \, \mathrm{d}y_k \right) \nabla^2_{y_k,y_\ell} \log p_1(\xi_{N,j_{-m:u}}) \, (y_\ell - \xi_{N,j_\ell}) \\
&\qquad\qquad \times p_0(y_{-m:k-1}, \xi_{N,j_k}, y_{k+1:u}) \, \{\mathrm{d}y_i\}_{i\neq k} \\
&= 0 \,.
\end{aligned}$$

Using (4.25) and Assumption 4.3-3), we find a bound for the remainder term:

$$\begin{aligned}
&\Bigg| \sum_{j_{-m:u}} \int\cdots\int_{C_{N,j_{-m}}\times\cdots\times C_{N,j_u}} (y_k - \xi_{N,j_k})^{\mathrm{T}} \, \nabla^2_{y_k,y_\ell} \log p_1(\xi_{N,j_{-m:u}}) \\
&\qquad\qquad \times (y_\ell - \xi_{N,j_\ell}) \, \epsilon'_{N,k}(y_{-m:u}) \, \mathrm{d}y_{-m:u} \Bigg| \leq C_2 \, c' \left(\frac{C_d}{N^{1/d}} \right)^3 \,. \qquad \text{(F.10)}
\end{aligned}$$

This concludes the proof of Lemma F.2. □

Lemma F.3. *For each $k \in \{-m, \ldots, u\}$,*

$$\begin{aligned}
&\mathbb{E}_0\Big[(Y_k - Z_{N,k})^{\mathrm{T}} \, \nabla^2_{y_k} \log p_1(Z_{N,-m:u}) \, (Y_k - Z_{N,k}) \Big] \\
&\quad = \frac{1}{N^{2/d}} \, \mathbb{E}_0 \left[\mathit{Tr} \left(\nabla^2_{y_k} \log p_1(Z_{N,-m:u}) \frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}} \right) \frac{p_0(Y_{-m:k-1}, Z_{N,k}, Y_{k+1:u})}{p_0(Y_{-m:u})} \right] + \bar{\epsilon}'_{N,k} \,,
\end{aligned}$$

where $\left|\bar{\epsilon}'_{N,k}\right| \leq \frac{c'_2}{N^{3/d}}$.

Proof. For each k, we expand the expectation:

$$\begin{aligned}
&\mathbb{E}_0 \left[(Y_k - Z_{N,k})^{\mathrm{T}} \, \nabla^2_{y_k} \log p_1(Z_{N,-m:u}) \, (Y_k - Z_{N,k}) \right] \\
&= \sum_{j_{-m:u}} \int\cdots\int_{C_{N,j_{-m}}\times\cdots\times C_{N,j_u}} (y_k - \xi_{N,j_k})^{\mathrm{T}} \, \nabla^2_{y_k} \log p_1(\xi_{N,j_{-m:u}}) \, (y_k - \xi_{N,j_k}) \, p_0(y_{-m:u}) \, \mathrm{d}y_{-m:u}
\end{aligned}$$

Plugging expansion (F.9) into the above equation leads to a dominant term and a remainder. The study of the dominant term uses the same arguments as Lemma F.1. The final expression comes from the following equality:

$$\int_{C_{N,j}} (y-\xi_{N,j})^{\mathrm{T}} A\,(y-\xi_{N,j})\,\mathrm{d}y = \mathrm{Tr}\left(A\,M_{N,j}\right)\,V_{N,j}^{1+2/d}\,,$$

for any d-by-d matrix A, and the definition of the specific point density $\zeta_{N,j} = \frac{1}{NV_{N,j}}$.

Equation (F.10) is also valid when $k = \ell$ i.e., for the remainder considered here. This proves Lemma F.3. □

Gathering (4.32) and Lemmas F.1, F.2, F.3 results in

$$\begin{aligned} U_N(u) = &-\frac{1}{N^{2/d}}\sum_{k=-m}^{u}\mathbb{E}_0\left[\nabla_{y_k}\log p_1(Z_{N,-m:u})^{\mathrm{T}}\frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}}\,\frac{\nabla_{y_k}p_0(Y_{-m:k-1},Z_{N,k},Y_{k+1:u})}{p_0(Y_{-m:u})}\right]\\ &-\frac{1}{2N^{2/d}}\sum_{k=-m}^{u}\mathbb{E}_0\left[\mathrm{Tr}\left(\nabla_{y_k}^2\log p_1(Z_{N,-m:u})\frac{M_N(Y_k)}{\zeta_N(Y_k)^{2/d}}\right)\frac{p_0(Y_{-m:k-1},Z_{N,k},Y_{k+1:u})}{p_0(Y_{-m:u})}\right]\\ &+\bar{\epsilon}_N(u)\,, \end{aligned}$$

where $|\bar{\epsilon}_N(u)| \le c_U\frac{m^3}{N^{3/d}}$ for some constant c_U.

Expanding $\nabla_{y_k}p_0$ and p_0 once again, under Assumptions 4.3 and 4.4-2), it is straightforward to write the dominant term in a simple form i.e., replace each $Z_{N,k}$ by Y_k. From (4.23), the remainder term is a little-o of $N^{-2/d}$. This proves Lemma 4.7. □

F.3 Proof of Lemma 4.9

Equation (4.39) ensures that the following series converges:

$$\Sigma_N = \mathbb{E}_0\left[\mathcal{H}_{N,0}(Y_{-\infty:0})\right] + \sum_{k=-\infty}^{-1}\mathbb{E}_0\left[\mathcal{H}_{N,k}(Y_{-\infty:0}) - \mathcal{H}_{N,k}(Y_{-\infty:-1})\right]\,.$$

Using (4.36), the approximation of $N^{2/d}(K-K_N)$ by series Σ_N leads to the following remainder:

$$\left|N^{2/d}(K-K_N) - \Sigma_N\right| \le \sum_{k=-m}^{0}\mathbb{E}_0\left|\Delta_N^{(k)}\right| + \sum_{k=-\infty}^{-m-1}\mathbb{E}_0\left|\Upsilon_N^{(k)}\right| + \check{\epsilon}_N\,, \tag{F.11}$$

where $\Delta_N^{(0)} = \mathcal{H}_{N,0}(Y_{-m:0}) - \mathcal{H}_{N,0}(Y_{-\infty:0})$ and

$$\begin{aligned} \Delta_N^{(k)} &= \mathcal{H}_{N,k}(Y_{-m:0}) - \mathcal{H}_{N,k}(Y_{-m:-1}) - \mathcal{H}_{N,k}(Y_{-\infty:0}) + \mathcal{H}_{N,k}(Y_{-\infty:-1}) \quad (\forall\, k \le -1)\,,\\ \Upsilon_N^{(k)} &= \mathcal{H}_{N,k}(Y_{-\infty:0}) - \mathcal{H}_{N,k}(Y_{-\infty:-1}) \quad (\forall\, k \le -m-1)\,, \end{aligned}$$

and where $\check{\epsilon}_N \to 0$ as $N \to \infty$. Using the triangular inequality, we obtain for each $k \le -1$:

$$\mathbb{E}_0\left|\Delta_N^{(k)}\right| \le \mathbb{E}_0\left|\mathcal{H}_{N,k}(Y_{-m:0}) - \mathcal{H}_{N,k}(Y_{-\infty:0})\right| + \mathbb{E}_0\left|\mathcal{H}_{N,k}(Y_{-m:-1}) - \mathcal{H}_{N,k}(Y_{-\infty:-1})\right|\,.$$

Using (4.38), this leads to:

$$\mathbb{E}_0\big|\Delta_N^{(k)}\big| \leq 2\, c_h \varphi_{m-|k|}\ .$$

From the triangular inequality once again,

$$\mathbb{E}_0\big|\Delta_N^{(k)}\big| \leq \mathbb{E}_0\left|\mathcal{H}_{N,k}(Y_{-m:0}) - \mathcal{H}_{N,k}(Y_{-m:-1})\right| + \mathbb{E}_0\left|\mathcal{H}_{N,k}(Y_{-\infty:0}) - \mathcal{H}_{N,k}(Y_{-\infty:-1})\right|\ .$$

Using (4.39), this leads to:

$$\mathbb{E}_0\big|\Delta_N^{(k)}\big| \leq 2\, c_h \psi_{|k|}\ .$$

After some algebra, there exists a constant c_Δ such that:

$$\begin{aligned}
\sum_{k=-m}^{-1} \mathbb{E}_0\big|\Delta_N^{(k)}\big| &\leq c_\Delta \sum_{k=-m}^{-1} \varphi_{m-|k|} \wedge \psi_{|k|} \\
&\leq c_\Delta \left(\sum_{k=-\lfloor m/2\rfloor}^{-1} \varphi_{m-|k|} + \sum_{k=-m}^{-\lfloor m/2\rfloor} \psi_{|k|} \right) \\
&\leq c_\Delta \left(\sum_{k=\lceil m/2\rceil}^{\infty} \varphi_k + \sum_{k=\lfloor m/2\rfloor}^{\infty} \psi_k \right) \\
&\leq c_\Delta\, \mathcal{T}_\Delta^{(m)}\ ,
\end{aligned}$$

Where $(\mathcal{T}_\Delta^{(m)})_{m\geq 0}$ is a sequence of positive numbers such that $\mathcal{T}_\Delta^{(m)} \to 0$ as $m \to \infty$. The last line of the above equation holds true under Assumption 4.4-4) since $\sum \varphi_k$ and $\sum \psi_k$ are convergent series. Similarly, $\mathbb{E}_0\big|\Delta_N^{(0)}\big| \leq\ c_h \varphi_m$.

The last series in (F.11) can be bounded using (4.39):

$$\sum_{k=-\infty}^{-m-1} \mathbb{E}_0\big|\Upsilon_N^{(k)}\big| \leq c_h \sum_{k=-\infty}^{-m-1} \psi_{|k|} = c_\Upsilon\, \mathcal{T}_\Upsilon^{(m)}\ ,$$

for some constant c_Υ and a given sequence $(\mathcal{T}_\Upsilon^{(m)})_{m\geq 0}$ such that $\mathcal{T}_\Upsilon^{(m)} \to 0$ as $m \to \infty$.

Putting all pieces together, (F.11) leads to:

$$\left|N^{2/d}(K - K_N) - \Sigma_N\right| \leq c_h \varphi_m + c_\Delta\, \mathcal{T}_\Delta^{(m)} + c_\Upsilon\, \mathcal{T}_\Upsilon^{(m)} + \check{\epsilon}_N\ .$$

The r.h.s. of the above inequality tends to zero as $m, N \to \infty$. This proves Lemma 4.9. □

Part IV

Bibliographie

–

Bibliography

[1] "Special issue on information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2405–2818, 2008. (cited on pp. 29, 34, 133, 138, 166)

[2] R. Ahlswede and I. Csiszàr, "Hypothesis testing with communication constraints," *IEEE Trans. Inf. Theory*, vol. 32, no. 4, pp. 533–542, 1986. (cited on pp. 27, 131)

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography–Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993. (cited on pp. 34, 139)

[4] R. Ahlswede and J. Korner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, 1975. (cited on pp. 27, 34, 35, 131, 138, 139, 146)

[5] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002. (cited on pp. 28, 83, 131, 197)

[6] A. Barron, "The strong ergodic theorem for densities: Generalized Shannon–McMillan–Breiman theorem," *Ann. Probab.*, vol. 13, no. 4, pp. 1292–1303, 1985. (cited on pp. 25, 129)

[7] G. Benitz and J. Bucklew, "Asymptotically optimal quantizers for detection of i.i.d. data," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 316–325, 1989. (cited on pp. 84, 109, 198, 228)

[8] W. Bennett, "Spectra of quantized signals," *Bell System Technical Journal*, vol. 27, pp. 446–472, 1948. (cited on pp. 25, 32, 84, 85, 92, 93, 129, 135, 198, 199, 206, 208, 210)

[9] T. Berger, "Multiterminal source coding," in *The information theory approach to communications*, G. Longo, Ed. Springer-Verlag, 1977, pp. 170–231. (cited on pp. 27, 34, 35, 38, 40, 41, 131, 138, 139, 143, 144, 145)

[10] T. Berger and J. Gibson, "Lossy source coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2693–2723, 1998. (cited on pp. 28, 132)

[11] T. Berger, K. Housewright, J. Omura, S. Yung, and J. Wolfowitz, "An upper bound on the rate distortion function for source coding with partial side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 25, no. 6, pp. 664–666, 1979. (cited on pp. 35, 40, 55, 138, 139, 144, 163)

[12] T. Berger and R. Yeung, "Multiterminal source encoding with one distortion criterion," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 228–236, 1989. (cited on pp. 34, 138)

[13] T. Berger, Z. Zhang, and H. Viswanathan, "The CEO problem," *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 887–902, 1996. (cited on pp. 112, 231, 232)

[14] A. Bhattacharyya, "On a measure of divergence between two statistical populations defined by their probability distributions," *Bull. Calcutta Math. Soc*, vol. 35, no. 99-109, p. 4, 1943. (cited on pp. 113, 235)

[15] P. Bianchi and J. Jakubowicz, "Adaptive learning vector quantization for on-line maximum likelihood estimation," *Work in progress*, 2011. (cited on pp. 113, 122, 233, 234, 235)

[16] P. Billingsley, *Probability and Measure (3rd Ed)*. John Wiley & Sons, 1995. (cited on pp. 23, 101, 127, 219)

[17] M. Bloch and J. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. Allerton*, 2008, pp. 818–825. (cited on pp. 138, 166)

[18] ——, "Secrecy from resolvability," *arXiv cs.IT*, arXiv:1105.5419v1, pp. 1–55, 2011. (cited on pp. 29, 133)

[19] D. Bosq, *Nonparametric statistics for stochastic processes: estimation and prediction*. Springer Verlag, 1998. (cited on p. 209)

[20] R. Bradley, "Basic properties of strong mixing conditions. a survey and some open questions," *Probab. Surv.*, vol. 2, pp. 107–144, 2005. (cited on pp. 89, 203, 209)

[21] L. Breiman, "The individual ergodic theorem of information theory," *Ann. Math. Stat.*, vol. 28, no. 3, pp. 809–811, 1957. (cited on pp. 25, 129)

[22] F. Bullo, J. Cortés, and S. Martinez, *Distributed control of robotic networks*. Princeton University Press, 2009. (cited on pp. 28, 132)

[23] O. Cappé, E. Moulines, and T. Ryden, *Inference in Hidden Markov Models*. Springer series in statistics, 2007. (cited on pp. 101, 102, 113, 219, 220, 235)

[24] J.-F. Chamberland and V. Veeravalli, "How dense should a sensor network be for detection with correlated observations?" *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5099–5106, 2006. (cited on pp. 85, 199)

[25] B. Chen, L. Tong, and P. Varshney, "Channel-aware distributed detection in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 1053, no. 5888/06, pp. 16–26, 2006. (cited on pp. 83, 197)

[26] J. Chen and T. Berger, "Successive Wyner–Ziv coding scheme and its application to the quadratic Gaussian CEO problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1586–1603, 2008. (cited on p. 232)

[27] P.-N. Chen, "General formulas for the Neyman–Pearson type-II error exponent subject to fixed and exponential type-I error bounds," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 316–323, 1996. (cited on pp. 88, 109, 202, 228)

[28] Y. Chen and A. Han Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, 2008. (cited on pp. 138, 166)

[29] J. Conway and N. Sloane, *Sphere packings, lattices, and groups (3rd Ed)*. Springer-Verlag, 1999. (cited on pp. 95, 212)

[30] M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, 1983. (cited on pp. 78, 191)

[31] T. Cover and J. Thomas, *Elements of information theory (2nd Ed)*. Wiley-Interscience, 2006. (cited on pp. 25, 51, 76, 85, 129, 159, 189, 198, 264, 272)

[32] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978. (cited on pp. 27, 31, 34, 50, 58, 59, 61, 62, 63, 65, 66, 81, 131, 134, 138, 158, 166, 167, 169, 170, 171, 173, 177, 183, 194, 247, 278)

[33] I. Csiszar and J. Korner, "Towards a general theory of source networks," *IEEE Trans. Inf. Theory*, vol. 26, no. 2, pp. 155–165, 1980. (cited on pp. 34, 138)

[34] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Akadémiai Kiado, Budapest, 1982. (cited on pp. 26, 28, 130, 132, 243, 244)

[35] A. Dembo and O. Zeitouni, *Large deviations techniques and applications (2nd Ed)*. Springer Verlag, 1998. (cited on pp. 109, 228)

[36] A. Detti and N. Blefari-Melazzi, "Network layer solutions for a content-centric internet," *Trustworthy Internet*, pp. 359–369, 2011. (cited on pp. 28, 132)

[37] R. Douc, E. Moulines, and T. Ryden, "Asymptotic properties of the maximum likelihood estimator in autoregressive models with Markov regime," *Ann. Stat.*, vol. 32, no. 5, pp. 2254–2304, 2004. (cited on pp. 101, 102, 219, 220)

[38] P. Doukhan, *Mixing: properties and examples*. Springer, 1994. (cited on p. 209)

[39] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, 2011. (cited on p. 195)

[40] ——, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, 2011. (cited on pp. 138, 166)

[41] ——, "Secure lossy transmission of vector gaussian sources," in *Proc. ISIT*, 2011. (cited on pp. 112, 230)

[42] A. El Gamal and Y.-H. Kim, *Lecture Notes on Network Information Theory*, arXiv:1001.3404v4, 2010. (cited on pp. 41, 145, 244, 248, 252)

[43] T. Flynn and R. Gray, "Encoding of correlated observations," *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 773–787, 1987. (cited on pp. 112, 231)

[44] N. Freris, H. Kowshik, and P. Kumar, "Fundamentals of large sensor networks: Connectivity, capacity, clocks, and computation," *Proc. IEEE*, vol. 98, no. 11, pp. 1828–1846, 2010. (cited on pp. 27, 131)

[45] Y. Gao and E. Tuncel, "New hybrid digital/analog schemes for transmission of a Gaussian source over a Gaussian channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6014–6019, 2010. (cited on pp. 58, 166)

[46] E. Gassiat and S. Boucheron, "Optimal error exponents in hidden Markov models order estimation," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 964–980, 2003. (cited on pp. 113, 235)

[47] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: lossy source-channel communication revisited," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1147–1158, 2003. (cited on pp. 58, 80, 166, 193)

[48] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Probl. Control Inf. Theory*, vol. 9, pp. 19–31, 1980. (cited on pp. 70, 72, 181)

[49] A. Gersho, "Asymptotically optimal block quantization," *IEEE Trans. Inf. Theory*, vol. 25, no. 4, pp. 373–380, 1979. (cited on pp. 94, 211)

[50] A. Gersho and R. Gray, *Vector quantization and signal compression*. Kluwer, 1992. (cited on pp. 84, 93, 198, 210)

[51] V. Girardin, *On the different extensions of the ergodic theorem of information theory*. Springer, 2005, ch. 7, pp. 163–179. (cited on pp. 25, 129)

[52] J. Goblick, T., "Theoretical limitations on the transmission of data from analog sources," *IEEE Trans. Inf. Theory*, vol. 11, no. 4, pp. 558–567, 1965. (cited on pp. 80, 193)

[53] S. Graf and H. Luschgy, *Foundations of quantization for probability distributions*. Springer, 2000. (cited on pp. 25, 109, 129, 228)

[54] R. Gray and D. Neuhoff, "Quantization," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2325–2383, 1998. (cited on pp. 25, 84, 91, 93, 94, 95, 111, 129, 198, 204, 206, 210, 211, 212, 229)

[55] D. Gündüz, E. Erkip, and H. Poor, "Lossless compression with security constraints," in *Proc. ISIT*, 2008, pp. 111–115. (cited on pp. 35, 139, 157)

[56] ——, "Secure lossless compression with side information," in *Proc. ITW*, 2008, pp. 169–173. (cited on pp. 35, 139, 157)

[57] D. Gündüz, J. Nayak, and E. Tuncel, "Wyner-Ziv coding over broadcast channels using hybrid digital/analog transmission," in *Proc. ISIT*, 2008. (cited on pp. 58, 166)

[58] D. Guo, S. Shamai, and S. Verdu, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, 2005. (cited on p. 195)

[59] ——, "Estimation of non-Gaussian random variables in Gaussian noise: Properties of the MMSE," in *Proc. ISIT*, 2008, pp. 1083–1087. (cited on p. 195)

[60] R. Gupta, "Quantization strategies for low-power communications," Ph.D. dissertation, The University of Michigan, 2001. (cited on p. 212)

[61] R. Gupta and A. Hero, "High-rate vector quantization for detection," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 1951–1969, 2003. (cited on pp. 32, 84, 85, 86, 89, 90, 91, 93, 94, 95, 102, 104, 107, 108, 109, 135, 198, 199, 200, 203, 205, 206, 208, 211, 212, 220, 222, 226, 228, 235)

[62] W. Hachem, E. Moulines, and F. Roueff, "Error exponents for Neyman-Pearson detection of a continuous-time Gaussian Markov process from regular or irregular samples," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3899–3914, 2011. (cited on pp. 85, 101, 199, 219)

[63] T. Han and K. Kobayashi, "A unified achievable rate region for a general class of multiterminal source coding systems," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 277–288, 1980. (cited on pp. 34, 138)

[64] T. Han and S. Amari, "Statistical inference under multiterminal data compression," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2300–2324, 1998. (cited on pp. 84, 198)

[65] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *Proc. ISIT*, 2010, pp. 2538–2542. (cited on pp. 34, 139, 166)

[66] C. Heegard and T. Berger, "Rate distortion when side information may be absent," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 727–734, 1985. (cited on pp. 34, 138)

[67] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002. (cited on pp. 28, 132)

[68] *Security architecture for Open Systems Interconnection for CCITT applications*, The International Telegraph and Telephone Consultative Committee, CCITT Rec. X.800, 1991. (cited on pp. 26, 27, 30, 130, 133)

[69] *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*, ISO/IEC Joint Technical Committee for Information Technology, ISO/IEC 7498-1, 1994. (cited on pp. 26, 130)

[70] S. Jana and R. Blahut, "Partial side information problem: Equivalence of two inner bounds," in *Proc. CISS*, 2008, pp. 1005–1009. (cited on pp. 40, 138, 144)

[71] N. Johnson, S. Kotz, and N. Balakrishnan, *Continuous univariate distributions, vol. 1 (2nd Ed)*. Wiley-Interscience, 1994. (cited on pp. 104, 222)

[72] A. Kaspi and T. Berger, "Rate-distortion for correlated sources with partially separated encoders," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 828–840, 1982. (cited on pp. 34, 138)

[73] A. Kaspi, "Rate-distortion function when side-information may be present at the decoder," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2031–2034, 1994. (cited on pp. 34, 138)

[74] S. Kassam, "Optimum quantization for signal detection," *IEEE Trans. Commun.*, vol. 25, no. 5, pp. 479–484, 1977. (cited on pp. 84, 198)

[75] S. Kay, *Fundamentals of statistical signal processing, vol. I Estimation Theory*. Prentice Hall PTR, 1993. (cited on pp. 113, 233)

[76] ——, *Fundamentals of statistical signal processing, vol. II Detection Theory*. Prentice Hall PTR, 1998. (cited on pp. 31, 135)

[77] K. Kittichokechai, T. J. Oechtering, and M. Skoglund, "Secure source coding with action-dependent side information," in *Proc. ISIT*, 2011. (cited on pp. 112, 122, 230)

[78] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. ITW*, 2009, pp. 95–99. (cited on pp. 138, 166)

[79] A. Kolmogorov, *Foundations of the theory of probability (2nd Ed)*. Chelsea Publishing Company, 1956. (cited on pp. 23, 127)

[80] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 4–21, 2003. (cited on p. 245)

[81] S. Kullback, *Information theory and statistics*. Dover, 1978. (cited on pp. 31, 113, 135, 235)

[82] H. Kushner and G. Yin, *Stochastic approximation and recursive algorithms and applications (2nd Ed)*. Springer-Verlag, 2003. (cited on p. 234)

[83] S. Lang, *Calculus of several variables*. Addison-Wesley, 1973. (cited on p. 293)

[84] A. Lapidoth and S. Tinguely, "Sending a bivariate Gaussian over a Gaussian MAC," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2714 –2752, 2010. (cited on pp. 72, 184)

[85] J. Lasserre, "A trace inequality for matrix product," *IEEE Trans. Autom. Control*, vol. 40, no. 8, pp. 1500 –1501, 1995. (cited on p. 213)

[86] E. Lehmann and G. Casella, *Theory of point estimation (2nd Ed)*. Springer New York, 1998. (cited on pp. 23, 127, 234)

[87] E. Lehmann and J. Romano, *Testing Statistical Hypotheses (3rd Ed)*. Springer Texts in Statistics, 2005. (cited on pp. 23, 84, 127, 198)

[88] Y. Li, M. Thai, and W. Wu, Eds., *Wireless Sensor Networks and Applications*. Springer-Verlag, 2007. (cited on pp. 28, 132)

[89] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008. (cited on pp. 34, 138, 166)

[90] ——, *Information theoretic security*. Now Publishers, 2009. (cited on pp. 29, 34, 50, 62, 66, 73, 133, 138, 158, 166, 170, 172, 173, 177, 182, 183, 186, 187, 251, 278)

[91] S. H. Lim, P. Minero, and Y.-H. Kim, "Lossy communication of correlated sources over multiple access channels," in *Proc. Allerton*, 2010. (cited on pp. 58, 72, 166, 184, 185, 280)

[92] P. Lima and L. Custdio, *Multi-Robot Systems*, ser. Studies in Computational Intelligence. Springer Berlin/Heidelberg, 2005, ch. 1, pp. 1–64. (cited on pp. 28, 132)

[93] Y. Linde, A. Buzo, and R. Gray, "An algorithm for vector quantizer design," *IEEE Trans. Commun.*, vol. 28, no. 1, pp. 84–95, 1980. (cited on pp. 26, 95, 130, 212)

[94] J. Liu, *Monte Carlo strategies in scientific computing*. Springer Verlag, 2001. (cited on pp. 105, 223)

[95] R. Liu and W. Trappe, Eds., *Securing wireless communications at the physical layer*. Springer, 2010. (cited on pp. 29, 34, 133, 138, 157, 166)

[96] R. Liu, Y. Liang, H. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. ITW*, 2007, pp. 337–342. (cited on pp. 34, 138, 166)

[97] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information-theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1839–1851, 2007. (cited on pp. 55, 163)

[98] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, 2002. (cited on pp. 34, 138)

[99] S. Lloyd, "Least squares quantization in PCM," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 129–137, 1982. (cited on pp. 26, 130)

[100] A. Lozano, A. Tulino, and S. Verdu, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3033–3051, 2006. (cited on p. 195)

[101] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. ISIT*, 2010, pp. 913–917. (cited on pp. 139, 166)

[102] A. Marshall and I. Olkin, *Inequalities: theory of majorization and its applications*. Academic Press New York, 1979. (cited on p. 213)

[103] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993. (cited on pp. 34, 139)

[104] B. McMillan, "The basic theorems of information theory," *Ann. Math. Stat.*, vol. 24, no. 2, pp. 196–219, 1953. (cited on pp. 25, 129)

[105] N. Merhav, "On the Shannon cipher system with a capacity-limited key-distribution channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1269–1273, 2006. (cited on pp. 35, 139)

[106] ——, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, 2008. (cited on pp. 27, 35, 55, 58, 63, 131, 139, 163, 166, 171)

[107] N. Merhav and S. Shamai, "On joint source-channel coding for the Wyner-Ziv source and the Gel'fand-Pinsker channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2844 – 2855, 2003. (cited on pp. 58, 166)

[108] V. Misra, V. K. Goyal, and L. R. Varshney, "Distributed scalar quantization for computing: High-resolution analysis and extensions," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5298–5325, 2011. (cited on pp. 27, 84, 131, 198)

[109] U. Mittal and N. Phamdo, "Hybrid digital-analog (HDA) joint source-channel codes for broadcasting and robust communications," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1082–1102, 2002. (cited on pp. 58, 166)

[110] S. Moy, "Generalizations of Shannon–McMillan theorem," *Pacific J. Math.*, vol. 11, no. 2, pp. 705–714, 1961. (cited on pp. 25, 129, 203, 204)

[111] S. Na and D. Neuhoff, "Bennett's integral for vector quantizers," *IEEE Trans. Inf. Theory*, vol. 41, no. 4, pp. 886–900, 1995. (cited on pp. 26, 32, 84, 85, 90, 91, 92, 95, 129, 135, 198, 199, 205, 206, 208, 212)

[112] C. Nair, "Capacity regions of two new classes of 2-receiver broadcast channels," in *Proc. ISIT*, 2009, pp. 1839–1843. (cited on pp. 68, 179)

[113] ——, "Capacity regions of two new classes of two-receiver broadcast channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4207–4214, 2010. (cited on pp. 52, 160)

[114] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *IEEE Symposium on Security and Privacy*, 2008, pp. 111–125. (cited on pp. 113, 233)

[115] ——, "De-anonymizing social networks," in *IEEE Symposium on Security and Privacy*, 2009, pp. 173–187. (cited on pp. 113, 233)

[116] D. Neuhoff, "On the asymptotic distribution of the errors in vector quantization," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 461–468, 1996. (cited on pp. 94, 211)

[117] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *arXiv cs.IT*, arXiv:1103.4086v1, pp. 1–40, 2011. (cited on pp. 138, 166)

[118] B. Oliver, J. Pierce, and C. Shannon, "The philosophy of PCM," *Proc. IRE*, vol. 36, no. 11, pp. 1324–1331, 1948. (cited on pp. 25, 129)

[119] Y. Oohama, "Gaussian multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1912 –1923, 1997. (cited on pp. 34, 35, 51, 52, 55, 138, 140, 159, 160, 163)

[120] ——, "The rate-distortion function for the quadratic Gaussian CEO problem," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1057 –1070, 1998. (cited on pp. 112, 231, 232)

[121] ——, "Rate-distortion theory for Gaussian multiterminal source coding systems with several side informations at the decoder," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2577–2593, 2005. (cited on pp. 112, 163, 231)

[122] P. Panter and W. Dite, "Quantization distortion in pulse-count modulation with nonuniform spacing of levels," *Proc. IRE*, vol. 39, no. 1, pp. 44–48, 1951. (cited on pp. 25, 129, 210)

[123] J. Pearl, "Fusion, propagation, and structuring in belief networks," *Artificial intelligence*, vol. 29, no. 3, pp. 241–288, 1986. (cited on p. 245)

[124] F. Perez-Cruz, M. Rodrigues, and S. Verdu, "MIMO Gaussian channels with arbitrary inputs: Optimal precoding and power allocation," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1070–1084, 2010. (cited on p. 195)

[125] K. Perlmutter, S. Perlmutter, R. Gray, R. Olshen, and K. Oehler, "Bayes risk weighted vector quantization with posterior estimation for image compression and classification," *IEEE Trans. Image Process.*, vol. 5, no. 2, pp. 347–360, 1996. (cited on pp. 84, 198)

[126] H. Permuter and T. Weissman, "Source coding with a side information "vending machine"," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4530–4544, 2011. (cited on pp. 112, 230)

[127] H. Permuter, Y. Steinberg, and T. Weissman, "Two-way source coding with a helper," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2905–2919, 2010. (cited on p. 245)

[128] B. Picinbono and P. Duvaut, "Optimum quantization for detection," *IEEE Trans. Commun.*, vol. 36, no. 11, pp. 1254–1258, 1988. (cited on pp. 84, 198)

[129] H. Poor, "Fine quantization in signal detection and estimation," *IEEE Trans. Inf. Theory*, vol. 34, no. 5, pp. 960–972, 1988. (cited on pp. 84, 113, 198, 233, 235)

[130] H. Poor and J. Thomas, "Applications of Ali–Silvey distance measures in the design of generalized quantizers for binary decision systems," *IEEE Trans. Commun.*, vol. 25, no. 9, pp. 893–900, 1977. (cited on pp. 84, 198)

[131] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. ITW*, 2007, pp. 442–447. (cited on pp. 35, 139, 155)

[132] S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, 2003. (cited on pp. 34, 138)

[133] J. Proakis and M. Salehi, *Digital communications (5th Ed)*. McGraw-Hill, 2007. (cited on pp. 23, 103, 127, 222)

[134] M. Rahman and A. Wagner, "Rate region of the Gaussian scalar-help-vector source-coding problem," in *Proc. ISIT*, 2010, pp. 56–60. (cited on pp. 34, 138, 163)

[135] C. Rasmussen and C. Williams, *Gaussian processes for machine learning*. MIT Press, 2006. (cited on p. 282)

[136] O. Rioul, "Information theoretic proofs of entropy power inequalities," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 33–55, 2011. (cited on pp. 55, 163)

[137] L. Sankar, S. Rajagopalan, and H. Poor, "A theory of privacy and utility in databases," *arXiv cs.IT*, arXiv:1102.3751v1, pp. 1–35, 2011. (cited on pp. 113, 233)

[138] S. Servetto, "Lattice quantization with side information: Codes, asymptotics, and applications in sensor networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 714 –731, 2007. (cited on pp. 34, 138)

[139] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948. (cited on pp. 17, 24, 26, 27, 29, 58, 59, 63, 121, 128, 130, 131, 133, 166, 167, 171, 248)

[140] ——, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949. (cited on pp. 29, 30, 34, 58, 133, 138, 166)

[141] ——, "Coding theorems for a discrete source with a fidelity criterion," *IRE International Convention Record*, vol. 7, pp. 325–350, 1959. (cited on pp. 28, 132)

[142] M. Skolnik, *Radar handbook (3rd Ed)*. McGraw-Hill, 2008. (cited on pp. 23, 127)

[143] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973. (cited on pp. 27, 34, 49, 58, 131, 138, 157, 166)

[144] Y. Sung, L. Tong, and H. Poor, "Neyman–Pearson detection of Gauss–Markov signals in noise : closed-form error exponent and properties," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1354–1365, 2006. (cited on pp. 85, 101, 199, 219)

[145] Y. Sung, S. Misra, L. Tong, and A. Ephremides, "Signal processing for application-specific ad hoc networks," *IEEE Signal Process. Mag.*, vol. 23, no. 5, pp. 74–83, 2006. (cited on pp. 28, 132)

[146] A. Swami, Q. Zhao, Y.-W. Hong, and L. Tong, Eds., *Wireless Sensor Networks*. Wiley, 2007. (cited on pp. 28, 131)

[147] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Proc. Allerton*, 2009, pp. 1061–1068. (cited on pp. 35, 139, 146)

[148] S. Tavildar, P. Viswanath, and A. Wagner, "The Gaussian many-help-one distributed source coding problem," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 564–581, 2010. (cited on pp. 34, 138, 163)

[149] R. Tenney and N. Sandell, "Detection with distributed sensors," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 17, no. 4, pp. 501–510, 1981. (cited on pp. 84, 198)

[150] C. Tian and S. Diggavi, "On multistage successive refinement for Wyner–Ziv source coding with degraded side informations," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2946–2960, 2007. (cited on pp. 34, 138)

[151] ——, "Side-information scalable source coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5591–5608, 2008. (cited on pp. 34, 138)

[152] R. Timo, T. Chan, and A. Grant, "Rate distortion with side-information at many decoders," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5240 –5257, 2011. (cited on pp. 34, 138, 154)

[153] J. Tsitsiklis, "Decentralized detection by a large number of sensors," *Math. Control Signals Systems*, vol. 1, no. 2, pp. 167–182, 1988. (cited on pp. 27, 84, 131, 198)

[154] ——, "Extremal properties of likelihood-ratio quantizers," *IEEE Trans. Commun.*, vol. 41, no. 4, pp. 550–558, 1993. (cited on pp. 84, 198)

[155] E. Tuncel, "Slepian-Wolf coding over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, 2006. (cited on pp. 27, 58, 62, 81, 131, 166, 170, 195)

[156] J. Villard. (2011) FMG, a basic Matlab GUI for Fourier-Motzkin elimination. [Online]. Available: http://www.joffrey-villard.fr/FMG (cited on pp. 40, 44, 67, 74, 144, 152, 178, 187)

[157] A. Wagner, B. Kelly, and Y. Altug, "The lossy one-helper conjecture is false," in *Proc. Allerton*, 2009, pp. 716–723. (cited on p. 138)

[158] A. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, 2008. (cited on pp. 34, 138, 163)

[159] P. Walters, *An introduction to ergodic theory*. Springer, 1982. (cited on pp. 23, 127)

[160] P. Willett, P. Swaszek, and R. Blum, "The good, bad, and ugly: Distributed detection of a known signal in dependent Gaussian noise," *IEEE Trans. Signal Process.*, vol. 48, no. 12, pp. 3266–3279, 2000. (cited on pp. 85, 199)

[161] M. Wilson, K. Narayanan, and G. Caire, "Joint source channel coding with side information using hybrid digital analog codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 4922–4940, 2010. (cited on pp. 58, 81, 166)

[162] J. Wolfowitz, *Coding Theorems of Information Theory*. Springer-Verlag, 1964. (cited on p. 129)

[163] A. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 21, no. 3, pp. 294–300, 1975. (cited on pp. 34, 35, 138, 139, 146)

[164] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–Part I," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, 1973. (cited on pp. 247, 248)

[165] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. (cited on pp. 17, 27, 29, 30, 31, 34, 55, 58, 68, 121, 131, 133, 134, 138, 163, 166, 179)

[166] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976. (cited on pp. 27, 34, 35, 39, 42, 47, 48, 53, 58, 59, 63, 64, 131, 138, 139, 143, 155, 156, 161, 166, 167, 171, 173)

[167] J.-J. Xiao, A. Ribeiro, Z.-Q. Luo, and G. Giannakis, "Distributed compression-estimation using wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 23, no. 4, pp. 27–41, 2006. (cited on pp. 84, 198)

[168] E. Yair, K. Zeger, and A. Gersho, "Competitive learning and soft competition for vector quantizer design," *IEEE Trans. Signal Process.*, vol. 40, no. 2, pp. 294–309, 1992. (cited on pp. 113, 235)

[169] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 918–923, 1983. (cited on pp. 35, 139)

[170] ——, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. Inf. Theory*, vol. 34, no. 4, pp. 835–842, 1988. (cited on pp. 35, 139)

[171] ——, "Coding theorems for Shannon's cipher system with correlated source outputs, and common information," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 85–95, 1994. (cited on pp. 35, 139)

[172] ——, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, 1997. (cited on pp. 35, 139)

[173] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Inf. Theory*, vol. 42, no. 4, pp. 1152 –1159, 1996. (cited on pp. 94, 95, 211, 212)

[174] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002. (cited on pp. 34, 138)